مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۱۳ ، بهار ۱۳۹۸، ص ۳۲- ۲۲

ISSN: 2745-3673
http://www.Rcsj.ir

مجلـه‌ی علمی پژوهش در علوم رایانه (سال چهارم)
شماره ۱۳ / بهار ۱۳۹۸ / ص ۳۲- ۲۲

امنیت اینترنت اشیا: نقش چالش‌ها و کاربردها

توحید ساکت

گروه کامپیوتر، واحد میانه، دانشگاه آزاد اسلامی، میانه، ایران.

نام نویسنده مسئول:
توحید ساکت

چکیده

اینترنت اشیا فناوری جدیدی است که در آن قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت، فراهم می‌گردد. شبکه‌های اینترنت اشیا می‌توانند برای کاربردهای بسیاری در حوزه‌های مختلف صنعتی از جمله نظارت بر زیرساخت، خدمات شهری، کاربردهای نظارتی و امنیتی و غیره مورد استفاده قرار بگیرند. پرداختن به همه کاربردها و به خصوص چالش‌های امنیتی پیش‌روی اینترنت اشیا اغلب زمانبر است. لذا باتوجه به اهمیت کاربردها و چالش‌های موجود در حوزه اینترنت اشیا و باتوجه به این که تحقیقات گذشته بیشتر بر روی جنبه‌های دیگر اینترنت اشیا متمرکز شده‌اند و به بحث امنیت کمتر بها داده شده است در این مقاله امنیت اینترنت اشیا، کاربردها و چالش‌های موجود آورده خواهد شد. برای فناوری اینترنت اشیاء کاربردهای بسیاری را می‌توان متصور شد که فقط تعدادی از این کاربردها، عملیاتی شده‌اند. در آینده نه چندان دور اینترنت اشیاء در خانه‌های هوشمند، کارخانه‌های هوشمند، مزارع هوشمند، ادارات هوشمند، سیستم حمل و نقل هوشمند، بیمارستان‌های هوشمند، دانشگاه‌های هوشمند و غیره به کار گرفته خواهد شد. چهار مشکل اساسی اینترنت اشیا عباتند از: نقض حریم شخصی، امنیت، اعتماد بیش از اندازه بر فناوری و محرمانگی که آن را تهدید می‌کند. تضمین امنیت سرویس‌ها و کاربردهای اینترنت، فاکتور بسیار مهمی در ایجاد اعتماد در کاربران و بکارگیری این بستر می‌باشد. کاربران باید اطمینان داشته باشند که اینترنت، کاربردهای آن و تجهیزاتی که به آن متصل هستند، به اندازه کافی برای انجام فعالیت‌های آنلاین، در برابر تهدیداتی که وجود دارد، امن هستند.

واژگان کلیدی: اینترنت اشیا، امنیت، حریم خصوصی.

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۱۳ ، بهار ۱۳۹۸، ص ۳۲- ۲۲

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

برای فناوری اینترنت اشیا کاربردهای بسیاری را می‌توان متصور شد که فقط تعدادی از این کاربردها، عملیاتی شده‌اند. در آینده نه چندان دور اینترنت اشیا در خانه‌های هوشمند، کارخانه‌های هوشمند، مزارع هوشمند، ادارات هوشمند، سیستم حمل و نقل هوشمند، بیمارستان‌های هوشمند، دانشگاه‌های هوشمند و غیره به کار گرفته خواهد شد. اتصال اشیا به شبکه‌های کامپیوتری و اینترنت در حال رشد بالایی است و بشر برای مدیریت صحیح اتفاقات و منابع خود نیاز دارد تا اطلاعات را با استفاده سنسورهای مختلف، از این اشیا مختلف جمع آوری نموده و این اطلاعات را تحلیل نمایند و بر اساس این تحلیل ها، تصمیم گیری نمایند. اینترنت اشیا پدیده‌ای جدید در دنیای فناوری و ارتباطات است. به صورت خلاصه اینترنت اشیا فناوری جدیدی است که در آن قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت، فراهم می‌گردد. شبکه‌های حسگر بیسیم به عنوان یکی از بخش‌های پایه‌ای در اینترنت اشیا بوده که یک حوزه محبوب تحقیقاتی اعم از مانیتورینگ، کنترل محیط و مراقبت بدن و کاربردهای نظامی است. این شبکه به دلیل ابعاد کوچک و توان عملیاتی سخت افزاری و ارتباطی چالش‌های بسیاری را نیز دارد. بدیهی است که چالش‌های ذاتی این نوع شبکه، موجب ایجاد محدودیت در عملکردهای تجمیع، انتقال و ارتباطات بین گره‌ها و مسیریابی آنها نیز شده است [۱].

یکی از چالش‌های عمده ای که باید به منظور وارد کردن اینترنت اشیا به جهان واقعی بر طرف شود امنیت است. معماری‌های اینترنت اشیا قرار است با جمعیتی حدود میلیاردها اشیا سر و کار داشته باشد، که با یکدیگر و با دیگر نهادها، مانند انسان ها و یا نهادهای مجازی تعامل خواهند داشت. همه 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 اشیا تأثیر می گذارد. با این حال، حفاظت اینترنت اشیا 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 اشیا ممکن است گیج کننده باشند. تهدیداتی که می‌تواند بر نهادهای اینترنت اشیا تأثیر گذارد متعدد هستند، مانند حملات باهدف کانال های ارتباطی مختلف، تهدیدات فیزیکی، محرومیت از خدمات، ساخت هویت، و غیره. در نهایت، پیچیدگی ذاتی اینترنت اشیا، که در آن نهادهای ناهمگن متعدد واقع در زمینه های مختلف می‌توانند اطلاعات را با یکدیگر مبادله کنند، پیچیدگی های بیشتر طراحی و بکارگیری مکانیزم های امنیتی کارآمد، سازگار و مقیاس پذیر را می‌طلبد.

با وجود تمام مزایای بیان شده، به دلیل این‌که اشیا متصل به اینترنت هستند همانند کامپیوتر و موبایل‌های هوشمند آن‌ها نیز در معرض نفوذ غیرمجاز و هک شدن می‌باشند. به علت گستردگی افرادی که با مجموعه اینترنت اشیا در ارتباط خواهند بود در صورت هک شدن آنها، اثرات زیانبار و گسترده‌ای خواهد داشت. به دلیل عدم دقت و رعایت نکردن نکات ایمنی، موارد متعددی از هک کردن دوربین‌های مداربسته و امنیتی به‌منظور جاسوسی و یا وارد شدن به آن محیط و یا مشاهده فعالیت‌های حریم خصوصی افراد و منتشر کردن آن در اینترنت برای مشاهده همگان وجود دارد. امنیت و محرمانه بودن، مسایل مهمی برای کاربردهای اینترنت اشیا بوده و همچنان با چالش‌های بزرگی مواجه است. مهمترین مشکل مرتبط با امنیت در اینترنت اشیا، بحث احراز هویت و جامعیت داده‌ها است. از آنجایی که احراز هویت معمولا نیازمند وجود سرورها و زیرساخت‌های مناسب برای تبادل پیام میان اجزاء مختلف است، تأمین آن در اینترنت اشیا کار دشواری است [۲].

در این مقاله به بررسی جامع چالش‌ها و روش‌های تأمین امنیت اینترنت اشیا و کارایی این روش جهت برقراری امنیت در اینترنت اشیا خواهیم پرداخت و چالش‌های موجود را مشخص خواهیم کرد تا بهترین راهکارها جهت تأمین امنیت اشیا در اینترنت مشخص شوند. با توجه به اهمیت امنیت در حوزه اینترنت اشیا در آینده، در این تحقیق به مطالعه امنیت در این زمینه خواهیم پرداخت. در این مقاله مفاهیم اینترنت اشیا، کاربردهای اینترنت اشیا، چالش‌های پیش رو و موضوعات مرتبط با این مفاهیم را توضیح داده و در انتها به امنیت اینترنت اشیا و شکاف‌های موجود خواهیم پرداخت تا بهترین راهکارها جهت تأمین امنیت اشیا در اینترنت مشخص شوند.

پیشینه تحقیق

عاطفه فرازمند و سروش احمدی در تحقیقی با عنوان (اینترنت اشیا و کاربرد های آن) در سال ۱۳۹۴ بیان کردند که مهمترین عامل اینترنت اشیا، یکپارچگی چندین تکنولوژی و راهکار ارتباطی است. تکنولوژی‌های شناسایی و ردیابی، حسگرهای سیمی و بیسیم و شبکه‌های فعال، پروتکل‌های افزایش ارتباط (قسمتی از نسل بعدی ارتباطات است) و هوشمندی اشیا مهمترین قسمت‌های اینترنت اشیا هستند. در این بررسی دیدگاه‌های مختلف اینترنت اشیا بیان شده است [۱].

ادشیر بحرینی نژاد و سلمان طاهری زاده در تحقیقی با عنوان (راه حل برای اینترنت اشیا) در سال ۱۳۸۶ بیان کردند که راه حل‌های یکپارچه کردن با شبکه‌های حسگری بی‌سیم به همراه الگوریتمی نوآورانه و یکپارچه کردن با فناوری حسگر ارایه شده است که می‌توانند

ISSN: 2745-3673
http://www.Rcsj.ir

کیفیت زندگی همه جا حاضر بودن را به کمک اینترنت بهبود بخشند. این راه‌حل‌ها در حالی که مکمل یکدیگر هستند، کمک می‌کنند در هر زمان و در هر کجا با هر چیزی ارتباط برقرار کرد و به اطلاعات محیطی و وضعیت آن دست یافت. در نهایت نیز ترکیبی از این ۵ راه‌حل‌ها برای استفاده بهینه تر از امکانات موجود معرفی می‌شود. این فناوری‌ها به عنوان موضوعات مفید و لازم، فرصت‌های جدیدی را برای بشر فراهم می‌کنند و تأثیر مهمی در زندگی امروزی ما دارند و راه و روش مدیریت سیستم‌های ما را آسان و تغییر خواهند داد [۲].

رهنورد و محمدیان در سال ۱۳۸۸ نیز سیستم مدیریت دانش را سیستمی برای پوشش فرایند خلق، جمع آوری، سازماندهی، اشاعه و کاربرد دانش در سازمان یا هنر خلق ارزش از دارایی‌های نامشهود سازمان معرفی کردند و حمایت مدیر ارشد، الگوگیری، معماری دانش، درگیری افراد، زیرساخت سیستم‌های اطلاعاتی، راهبرد و اهداف، سنجش دانش، زیرساخت سازمانی، آموزش، منابع انسانی، ایجاد انگیزه، فرهنگ سازمان و کار تیمی را عوامل پایه‌ای برای موفقیت هر سیستم مدیریت دانش می‌دانند [۳].

مرکز تحقیقات مخابرات ایران (پژوهشگاه ارتباطات و فناوری اطلاعات) پروژه‌هایی را برای بررسی پیاده‌سازی فناوری اینترنت اشیا و امنیت آن در ایران انجام داده است. یکی از این پروژه‌ها با عنوان «تدوین کسب و کار اینترنت اشیا در کشور» انجام شده است. در این پروژه بر اساس تجربیات علمی و عملیاتی کشورهای مختلف در حوزه‌های حاکمیت، کسب و کار، کاربردها و فناوری‌ها مطالعات اولیه صورت گرفت و نقشه راه ایران با هدف استفاده ایران از فناوری‌های نوین نظیر اینترنت اشیا برای افزایش رفاه اقتصادی، کیفیت زندگی و حفاظت از محیط زیست برای رسیدن به چشم‌انداز اقتصادی ۱۴۰۴ تعیین شد [۴].

تحقیق انجام گرفته توسط حمیدرضا ارکیان و همکاران در سال ۱۳۹۴ نشان می دهد، علی‌رغم تحقیقات صورت گرفته مرتبط با اینترنت اشیا و امنیت آن، حملات مختلفی معرفی می‌شود که فضای این مفهوم و فناوری‌های مرتبط با آن را درگیر کرده است. این نشان می‌دهد که فناوری به پرتگاه بسیار پیچیده‌ای نزدیک شده‌است و اقدامات متقابل اغلب صرفاً واکنشی است؛ بنابراین نیاز است اندکی به عقب بازگردیم -زمانیکه این فناوری‌های مؤثر بر زندگی بشر، در حال توسعه بودند و به سمت ابعاد خوبی از فناوری تمایل داشتند- و امنیت را در هر سطحی بازتعریف کنیم. اگرچه این مسائل به خاطر اجبارهای نظارتی در حال تغییر است اما با این حال تأیید مراکز دولتی به معنای امنیت نخواهد بود. مسئله امنیت در اینترنت اشیا را می‌توان مهمترین چالش توسعه این فناوری در نظر گرفت. در این رابطه استانداردهای مختلفی در حال توسعه است ولی همچنان نیازمندی‌های امنیتی اینترنت چیزها و حتی مخاطرات آن به خوبی شناسایی و تحلیل نشده است. با بررسی مقالات و کتاب‌هایی که در حوزه امنیت اینترنت اشیا ارائه شده‌اند، می‌توان دریافت که امنیت باید در تمام سطوح بسته‌ها و سرویس‌ها نیز در نظر گرفته شود؛ بنابراین در تمام مراحل توسعه سیستم، ویژگی‌های امنیتی وجود خواهند داشت. به این نوع توسعه امنیت، رویکرد «دفاع در عمق» گفته می‌شود. این رویکرد، امنیت را در دل شبکه اینترنت چیزها گنجانده و به سازمان‌ها و شرکت‌ها اجازه می‌دهد تا با درگیر کردن مهاجمین به صورت لایه به لایه، زمان بیشتری برای دفاع از منابع خود داشته باشند [۵].

روش

در این مطالعه مروری، کلیه مقالات خارجی چاپ شده تا سال ۲۰۱۶ به زبان انگلیسی و مقالات فارسی تا سال ۱۳۹۶ که در زمینه چالش‌ها،کاربردها و امنیت اینترنت اشیا انجام شده بودند، مورد بررسی قرار گرفتند. این مطالعات از طریق بانک‌های اطلاعاتی Google Scholar، Ovid، Science Direct، PubMed، CINAHL و با استفاده از کلیدواژه‌های امنیت، اینترنت اشیا، حریم‌خصوصی، چالش‌ها و کاربردها به دست آمد. نتیجه‌ی این جستجو دستیابی به ۱۸ مقاله‌ی اصلی و مرتبط با موضوع بود که از این میان ۶ مقاله به علت دارا نبودن معیارهای ورود از مطالعه حذف و ۱۲ مطالعه وارد پژوهش شدند. شرایط ورود مقالات به مطالعه شامل کاربردهای اینترنت اشیا و چالش‌های امنیتی در آن بود که از میان آنها جمعاً ۱۲ تحقیق به عنوان منبع انتخاب شدند. این مقاله به صورت مروری ارایه شده و مطالب به روش کتابخانه‌ای گردآوری شده است، با هدف مروری بر چالش‌ها و کاربردهای مختلف اینترنت اشیا و دیگر مباحث مهم در این زمینه که قصد آگاه‌سازی هر چه بیشتر جامعه هدف را دارد. قسمت اول به توضیح کلی اینترنت اشیا، پیشینه مطالعات انجام شده و ارایه‌ی مقدمه‌ای جامع در این خصوص می‌پردازد. قسمت دوم روش را بیان می‌کند. قسمت سوم شامل یافته‌ها است که از مستندات منتخب فیش‌برداری شد و مطالب جمع‌آوری شده در دو حیطه "کاربردهای اینترنت اشیا" و "چالش‌های اینترنت اشیا"، تقسیم‌بندی و خلاصه‌سازی شد و در قسمت چهارم و انتهایی به بحث و نتیجه‌گیری پرداخته می‌شود.

ISSN: 2745-3673
http://www.Rcsj.ir

یافته‌ها

کاربردهای اینترنت اشیا

برای فناوری اینترنت اشیاء کاربردهای بسیاری را می‌توان متصور شد که فقط تعدادی از این کاربردها، عملیاتی شده‌اند. در آینده نه چندان دور اینترنت اشیاء در خانه‌های هوشمند، کارخانه‌های هوشمند، مزارع هوشمند، ادارات هوشمند، سیستم حمل و نقل هوشمند، بیمارستان‌های هوشمند، دانشگاه‌های هوشمند و غیره به کار گرفته خواهد شد که در ادامه به شرح آنها می‌پردازیم.

اینترنت اشیا در هوافضا

اینترنت اشیا با شناخت قطعات و محصولات جعلی باعث ایجاد امنیت و آرامش در زمینه سرویس‌های هوایی می‌شود. صنعت حمل و نقل هوایی در مقابل خطر قطعات تایید نشده و مشکوک، بسیار آسیب‌پذیر است. بنابراین قطعات غیر استاندارد به شدت امنیت یک هواپیما را به خطر می‌اندازند. علاوه براین، تجزیه و تحلیل مواد مورد استفاده در هواپیما بسیار وقت گیر می‌باشد. پیش از هر پرواز صحت قطعات هواپیما باید توسط بازرسین تایید شود. این کار مبتنی بر اسناد همراه هواپیما است که خود این اسناد می‌توانند جعلی باشند. حال این مشکل را می‌توان به وسیله تعریف یک دستورالعمل الکتریکی برای برخی قحعات خاص که دستور تولید، نگهداری، و استفاده از آن وسیله را شرح می‌دهد برطرف کرد. بنابراین با ذخیره سازی این دستورالعمل‌ها در پایگاه‌های داده غیر متمرکز که در مقابل سرقت امن هستند، قبل از نصب هر قطعه می‌توان از صحت و اصالت آن اطلاع کسب کرد [۶].

اینترنت اشیا در شبکه

شبکه‌های حسگر مبتنی بر اینترنت اشیا نسل جدیدی از شبکه‌ها هستند که به طور معمول از تعداد زیادی گره ارزانقیمت تشکیل شده اند و ارتباط این گره ها به صورت بیسیم صورت می‌گیرد. هدف اصلی در این شبکه‌ها، جمع آوری اطلاعاتی در محیط پیرامون حسگرهای شبکه است. نحوه عملکرد کلی این شبکه‌ها به این صورت است که گره ها اطلاعات مورد نیاز را جمع آوری می‌کنند و سپس آنها را به سمت گیرنده ارسال می کنند. آنچه امروزه استفاده از این شبکه‌ها را گسترش داده است گره های حسگر چندگانه، با توان مصرفی پایین و هزینه کم است که از نظر اندازه خیلی کوچک هستند و برای مسافت‌های کوتاه می‌توانند باهم ارتباط برقرار کنند. این گره های حسگر کوچک طبق نظریه شبکه‌های حسگر، دارای تجهیزات حس کردن، پردازش داده ها و مخابره آنها می‌باشند. شبکه‌های حسگر در واقع تجمع تعداد زیادی از گره های حسگر می باشند که در محیط پراکنده می شوند و هر کدام به طور خود مختار و با همکاری سایر گره ها هدف خاصی را دنبال می کنند. گره ها به هم نزدیک هستند و هر گره ای با گره دیگر می‌تواند ارتباط برقرار کند و اطلاعات خود را در اختیار گره دیگری قرار دهد و در نهایت وضعیت محیط تحت نظر، به یک گره مرکزی گزارش می شود. امروزه کاربردهای وسیعی برای این شبکه ها وجود دارد که از آن جمله می‌توان به اتوماسیون خانگی بیسیم مثل: کنترل روشنایی، مصرف انرژی هوشمند و غیره اشاره کرد [۷].

ISSN: 2745-3673
http://www.Rcsj.ir

دسته بندی اینترنت اشیا [۷].

اینترنت اشیا در صنعت خودرو

ماشین‌های پیشرفته، قطارها، اتوبوس‌ها و حتی دوچرخه‌ها در حال مجهز شدن به حسگرهایی با قدرت پردازش بالا هستند. از جمله کاربردهای اینترنت اشیا در صنعت خودرو می‌توان به کاربرد تجهیزات هوشمند در جهت مشاهده و گزارش پارامترهای متفاوت از فشار داخل تایرها گرفته تا تخمین فاصله از سایر وسایل در حال حرکت در جاده اشاره کرد. تجهیزات متصل شده به قطعات وسایل نقلیه شامل اطلاعاتی همچون نام تولید کننده و زمان و مکان تولید، شماره سریال، نوع کد تولید و نیز محل دقیق آن قطعه در هر وسیله نقلیه هستند [۶].

نسل آینده خودروها [۶]

اینترنت اشیا در داروسازی

برای محصولات دارویی، امنیت و ایمنی بیشترین اهمیت را دارد. در اینترنت اشیا با اتصال برچسب‌های هوشمند به مواد دارویی به راحتی می‌توان زنجیره تولید و عرضه آنها را کنترل و نظارت کرد. به عنوان مثال، اقلامی که نیاز به ذخیره‌سازی در شرایط خاص دارند مانند داروهایی که حتماً باید در دمای خاصی نگهداری شوند را می‌توان به طور مداوم نظارت کرد و در صورتی که این شرایط در طول حمل و

ISSN: 2745-3673
http://www.Rcsj.ir

نقل دارو نقض شود از ورود آنها به بازار خودداری نمود. از همه مهم‌تر آن که، به واسطه این فناوری می‌توان مواد دارویی جعلی را تشخیص داد. همچنین برچسب‌های هوشمند قادرند تا از طریق اعلام دستورالعمل‌های لازم جهت نگهداری، نحوه استفاده و تاریخ انقضای دارو به بیمار کمک بسیاری کنند [۶].

اینترنت اشیا در خرده فروشی

اینترنت اشیا می‌تواند چندین مزیت در خرده فروشی و مدیریت زنجیره تامین ارائه دهد. یک خرده فروش می‌تواند نیازمندی‌های کالاهای خود را به درستی مدیریت کند. همچنین اگر تولید کنندگان عمده، اطلاع از میزان نیاز خرده‌فروشان داشته باشند بهتر می‌توانند تولیدات خود را مدیریت کرده و وضعیت بازار را کنترل کنند. بنابراین با جمع‌آوری اطلاعات ارسال شده از نیازمندی‌های خرده‌فروشان، می‌توانند تولیدات خود را بهینه کنند. اینترنت اشیا می‌تواند یک پتانسیل عظیم جهت انبارسازی محصولات در خرده فروشی‌ها ایجاد کند. طبق آمار سالیانه حدود ۴,۰ درصد از فروش خرده‌فروشان به دلیل کمبود کالا از بین می‌رود. بنابراین این فناوری با نمایش لحظه‌ای میزان موجودی و فروش هر کالا قادر است نقش بزرگی در زنجیره تولید و عرضه کالاها ایفا کند [۶].

اینترنت اشیا در نظارت بر محیط زیست

استفاده از ابزارهای قابل شناسایی بیسیم در محیط زیست از دیگر مزایای اینترنت اشیا است که امکان نظارت تمام وقت محیط زیست و کنترل تغییرات انواع گونه‌های حیوانی و گیاهی را برای ما فراهم می‌کند. با استفاده از حسگرهایی که در سطح جنگل‌ها توزیع شده‌اند می‌توان از آتشسوزی‌های وسیع که سالانه در جنگل‌های جهان اتفاق می‌افتد، جلوگیری کرد. همچنین با بهره‌گیری از شبکه حسگرهای بیسیم که در سطح شهر پخش شده‌اند می‌توان به طور لحظه‌ای از میزان آلاینده‌های موجود در هوا، در نقاط مختلف شهر اطلاع دقیق پیدا کرد. دستگاه‌های مجهز به حسگرهای متفاوت، از نزدیک، مدام محیط زیست را نظارت می‌کنند و اطلاعات بسیاری از قبیل تغییرات در ساختار شهرها، جمع آوری اطلاعات در مورد فاضلاب‌ها، کیفیت هوا و دفع زباله‌ها را در اختیار ما قرار می‌دهند. مشاهده و اندازه‌گیری بسیاری از تغییرات زیست محیطی بسیار دشوار است و در واقع اینترنت اشیا با در اختیار قرار دادن اطلاعات جمع آوری شده در مورد این مشاهدات اولین قدم برای درک اثرات عوامل انسانی و غیر انسانی در ایجاد دگرگونی در محیط زیست برای ما فراهم می‌کند. از جمله مهم‌ترین کاربردهای اینترنت اشیا در این حوزه می‌توان به دستگاه‌های هوشمند کنترل لحظه‌ای هوای اطراف، سطل زباله‌های هوشمند و دستگاه‌های هوشمند مسیریابی دریایی اشاره کرد [۶].

اینترنت اشیا در شبکه برق

شبکه‌های هوشمند یک مورد خاص هستند. این شبکه‌ها در آینده با استفاده مکانیزه از اطلاعات تأمین‌کنندگان و مصرف‌کنندگان برق، به بهبود کارایی و قابلیت اطمینان اقتصادی در صنعت برق کمک می‌کنند. ۴۱۰۰۰ جستوجوی ماهانه در گوگل، برجسته بودن این موضوع را نشان می‌دهد. حسگرها برای سیستم‌های شبکه هوشمند ضروری هستند چرا که به اپراتورها این امکان را می‌دهند تا میزان استفاده و عملکرد شبکه را در هر لحظه اندازه بگیرند. این بدین معنی است که به جای اینکه منتظر تماس مشتریانی شوند که برق آنها قطع شده است، شرکت‌های تولید برق می‌توانند نقطه قطع برق را تشخیص داده و با تغییر مسیر انتقال توان و یا تولید تجهیزات جدید، جریان برق را به نقطه قطع شدگی هدایت کنند. مدیریت این حسگرها از کاربردهای اساسی و مهم اینترنت اشیاء می‌باشد. کنتورهای هوشمند و دارای قابلیت ارتباط دوطرفه می‌توانند زمان قطع انرژی را کاهش داده و تشخیص علت قطع شدگی را سریع‌تر کنند [۶].

اینترنت اشیا در سلامت الکترونیک

اینترنت اشیا در حوزه سلامت الکترونیک فرصت‌های زیادی ایجاد می‌کند. در واقع این فناوری می‌تواند خدمات سلامت را بهبود داده و منجر به نوآوری‌های مختلفی در این ارتباط شود. بکارگیری بستر ابری در کاربردهای حوزه سلامت اینترنت اشیا، راهکار کارایی برای مدیریت داده‌های جمع‌آوری شده از سنسورهای این حوزه است. در واقع جزئیات و پیچیدگی‌های فنی زیرساخت را از دید توسعه‌دهندگان کاربردهای سلامت مخفی می‌کند; همچنین جمع‌آوری و تجمیع داده را آسان تر و با هزینه کمتر فراهم می‌آورد. همچنین بستری مناسب برای کاربردهای سلامت مبتنی بر گوشی‌های موبایل می‌باشد. بستر ابری امکان روبرو شدن با چالش‌های معمول حوزه سلامت (همچون امنیت، حریم خصوصی و قابلیت اطمینان) را با افزایش امنیت داده‌های پزشکی و دسترس‌پذیری و افزونگی سرویس، فراهم می‌کند .به واسطه مدیریت کارای داده‌های جمع‌آوری شده در بستر ابری، ارائه بلادرنگ خدمات لازم برای ارتقاء کیفیت زندگی ممکن است. همچنین با بکارگیری بستر ابری می‌توان بر مشکل اجراء الگوریتم‌های سنگین داده‌کاوی و یادگیری ماشین بر روی تجهیزات (که محدودیت باتری و

ISSN: 2745-3673
http://www.Rcsj.ir

ظرفیت پردازشی دارند) غلبه کرده و سرویس‌های سلامت چندرسانه‌ای و امن را عرضه کرد. بستر ابری زیرساخت ذخیره‌سازی و پردازشی منعطفی را برای تحلیل‌های آنلاین و آفلاین جریان داده تولید شده در شبکه‌های سنسوری بدن فراهم می‌کند. از جمله چالش‌های عمومی حوزه سلامت، که لازم است بر روی آنها کار شود، می‌توان به عدم وجود اعتماد در امنیت و حریم خصوصی، غیرقابل پیش‌بینی بودن کارایی سیستم و کیفیت سرویس، موضوعات حقوقی مرتبط با مالکیت داده، اشاره کرد [۸].

اینترنت اشیا در شبکه بازیافت

از اینترنت می توان برای کنترل انتشار وسایل نقلیه جهت نظارت و کنترل بر آلودگی هوا، دسته بندی و غربال انواع زباله و استفاده مجدد از قطعات الکترونیکی و دفع انواع زباله استفاده کرد. در واقع این تجهیزات هوشمند هستند که با ارائه اطلاعات از انواع وسایل، کار شناختن و جداسازی زباله ها را برای ما میسر می‌سازند. همچنین این تجهیزات به کاهش زباله‌ها به خصوص زباله‌های الکترونیکی و نیز جلوگیری از انتشار زباله‌های خطرناک در محیط زیست کمک می‌کنند. تجهیزات هوشمند با برآورد نیازهای کاربران باعث کاهش حمل و نقل و در نتیجه کاهش میزان آلودگی می‌شوند و به صرفه جویی در وقت و هزینه بسیار کمک می‌کنند [۸].

اینترنت اشیا در پزشکی

دستگاه‌های اینترنت اشیا می‌تواند برای فعال کردن نظارت از راه دور بر سلامت و اخطارهای اضطراری استفاده شود. دستگاه نظارت بر سلامت از فشارخون و نظارت بر ضربان قلب تا دستگاه‌های پیشرفته قادر به نظارت ایمپلمنت‌های تخصصی، مانند ضربان‌ساز، مچ بندهای الکترونیکی یا سمعک پیشرفته را شامل می‌شود. بعضی از بیمارستان‌ها شروع به اجرای «تخت هوشمند» کرده‌اند که می‌تواند تشخیص دهد که تحت چه زمانی اشغال است یا زمانی که بیمار می‌خواهد بلند شود را متوجه می‌شود. همچنین می‌تواند فشار مناسب را تنظیم کند و بدون تعامل پرستاران، به بیمار رسیدگی شود. سنسورهای تخصصی همچنین می‌تواند فضاهای زندگی را برای نظارت بر سلامت و رفاه عمومی شهروندان، مجهز کند. در حالی که همچنین از اجرای درمان مناسب و کمک به مردم برای دوباره بدست آوردن پویایی به‌وسیله معالجه اطمینان حاصل کنند [۱۱].

اینترنت اشیا در خانه هوشمند

در یک خانه هوشمند وسایل الکتریکی درون خانه به یکدیگر متصلاند و از طریق اینترنت اشیاء قابلیت مدیریت آنها توسط ما کارآمدتر خواهد بود. تصور کنید که برای مسافرت از خانه خارج شدهاید و فراموش کرده باشید که چراغ های منزل را خاموش کنید و یا کنتور گاز و آب را قحع کنید. این لحظه همان موقعی است که اینترنت اشیاء به کمک شما می‌آید و به شما این امکان را می‌دهد تا از دور نیز بر وسایل و ابزارهای درون منزلتان مدیریت داشته باشید. و یا حتی در مواقعی که در منزل نیستید و قرار است سرقتی از منزلتان رخ دهد به صورت لحظه‌ای باخبر شده و پلیس را در جریان بگذارید [۶].

بکارگیری امکاناتی که خانه را در اصطلاح هوشمند می‌کند، همواره یکی از مواردی بوده است که بشر توجه زیادی به آن داشته و در طول دوره‌های مختلفِ توسعه ی فناوری راه حل‌های متعددی برای این منظور خلق کرده است. خانه هوشمند به خانه‌ای گفته می‌شود که ساکنین آن امکان تنظیم و کنترل تجهیزات الکترونیکی منزل خود را از راه دور و نزدیک داشته باشند و نیز بتوانند برنامه‌های مختلف و سناریوهای متنوعی را برای آن تجهیزات تعریف و اجرا نمایند.

به طور کلی تجهیز ساختمان به مجموعه تجهیزاتی که به منظور افزایش کارایی و بهره وری و ایجاد محیطی مطبوع برای ساکنین آن طراحی و اجرا میگردند، هوشمند سازی ساختمان نامیده می‌شود. هدف از اجرای پروژه های هوشمند سازی می‌تواند تبدیل فضا به یک فضای متمایز و لوکس، تبدیل ساختمان به یک ساختمان با مصرف بهینه انرژی و یا تبدیل خانه به یک خانه مدرن و امن با مدیریت هوشمند باشد.

با ورود سیستم‌های جدید از قبیل کنترل روشنایی، پرده، موتور خانه، اعلام حریق، کنترل دسترسی، دوربین مدار بسته و ... در ساختمانها و لزوم کنترل مرکزی آنها، وجود یک سیستم یکپارچه و قابل برنامه ریزی احساس می گردد [۱۲].

چالش‌های اینترنت اشیا

چهار مشکل اساسی ایده اینترنت اشیا را تهدید می‌کند؛ نقض حریم شخصی، امنیت، اعتماد بیش از اندازه بر فناوری و محرمانگی. اینها مشکلاتی هستند که همیشه وقتی همه چیز بر عهده اینترنت گذاشته می‌شود، وجود دارند. در خصوص حریم شخصی، اقدامات امنیتی

ISSN: 2745-3673
http://www.Rcsj.ir

وجود دارند که از اطلاعات شخصی حفاظت کنند، اما همیشه نیز این امکان برای هکرها وجود دارد که به سیستم‌های امنیتی نفوذ کنند و داده‌ها را به سرقت ببرند در ادامه این چالش‌ها را تشریح می‌کنیم.

چالش امنیت

امنیت ایده ای جهانی است که با ایمنی گره خورده است، و اطمینان یک شخص به زندگی اش بدون آسیب رسیدن به زندگی، ویژگی ها و حقوق آن می باشد. امنیت سایبری زیرمجموعه ای است که بر سیستم های محاسباتی، کانال های تبدیل داده ها و اطلاعاتی که پردازش می کنند، و تخطی از آنچه ممکن است طبق قوانین جنایی مجازات شوند تمرکز دارد. امنیت اطلاعات و اطمینان با امنیت سایبری با تمرکز بر اطلاعات پردازش شده در هم پیچیده شده است. علاوه بر این، مفاهیم حقوقی و اجتماعی "حق حفظ حریم خصوصی" شهروندان، با چالش امنیت سایبری و منافع شهر هوشمند در هم تنیده شده است. مفهوم قانونی/ اجتماعی حریم خصوصی به جنبه‌های محرمانه زندگی، کنترل مشخصات عمومی آن و یک زندگی عاری از دخالت بی جا اشاره دارد.

اقدامات لازم در خصوص حصول اطمینان از انعطاف معماری نسبت به حملات، تصدیق داده ها، کنترل دسترسی و حریم خصوصی مشتری باید انجام گردد. یک چارچوب قانونی مناسب در این تکنولوژی باید وجود داشته باشد و به بهترین شکل توسط قانونگذار بین المللی برقرار گردد تا توسط بخش خصوصی با توجه به نیازهای خاص پشتیبانی شود. محتویات قوانین مربوطه باید حق دسترسی به اطلاعات، مقررات منع یا محدود کردن استفاده از مکانیسم های اینترنت اشیا، برقراری قوانین امنیتی فناوری اطلاعات، مقررات حمایت از استفاده از مکانیسم های اینترنت اشیا و استقرار یک نیروی کار برای انجام تحقیقات بر روی چالش های اینترنت اشیا را در بر گیرد.

هدف قانون امنیت، محافظت از تهدیدات است. این تهدیدات به دو دسته طبقه بندی می شوند که عبارتند از: تهدیدات خارجی مانند حمله مهاجمان به تشکیلات سیستم و تهدیدات داخلی مانند سوء استفاده از سیستم و یا اطلاعات. سه عامل اصلی امنیت وجود دارد: محرمانه بودن اطلاعات، حفظ حریم خصوصی و اعتماد. محرمانه بودن اطلاعات 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 اشیا. اعتماد جهت اعمال قوانین امنیتی در سیستم تضمین شده است و نمونه رایج از اعتماد، گواهینامه های دیجیتال هستند. حریم خصوصی 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 حریم خصوصی در برنامه های کاربردی هستند، فن‌آوری های بهبود حریم خصوصی می تواند به موضوع اشیا، تراکنش یا سیستم متمایل گردد، و آن برای محافظت از هویت در اینترنت استفاده می شود. در محیط اینترنت اشیا، امنیت و حریم خصوصی برای تضمین یک تعامل قابل اعتماد بین دنیای فیزیکی و دنیای مجازی مهم هستند [۹].

چالش حریم‌خصوصی

به دلیل آنکه داده‌های بیشتری از منابع مختلف با استفاده از این دستگاه ها جمع آوری می شوند، اینترنت اشیا می تواند تأثیر قابل توجهی بر حریم خصوصی اشخاص با پتانسیل اضافی برای نظارت گسترده افراد بدون اطلاع یا رضایت آنها داشته باشد. به عبارتی، اینترنت اشیا، نوید بخش یک عصر جدید از محاسبات است که به موجب آن هر شی قابل تصور مجهز می شود، و یا به یک دستگاه هوشمند متصل می شود که اجازه جمع آوری داده ها و ارتباطات از طریق اینترنت را می دهد. اینترنت اشیا ، حریم خصوصی افراد را از نظر جمع آوری و استفاده از اطلاعات شخصی افراد به چالش می‌کشد.

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 اشیا از ضروریات محسوب می شود، به حوزه کاربری و فناوری های مورد استفاده در اینترنت اشیا برمی گردد. برنامه های کاربردی در بخش مراقبت‌های بهداشتی، بیانگر برجسته ترین حوزه کاربری هستند که در آن اطمینان یافتن از وجود امنیت در حوزه اطلاعات در فناوری اینترنت اشیا ضروری می نماید. به علاوه در چشم انداز اینترنت اشیا، 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 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 واقعی است که ممکن است توسعه اینترنت اشیا را با محدودیت مواجه سازد.

گیبس (۲۰۰۸) حریم خصوصی را به عنوان "محدودیت دسترسی دیگران به یک شخص" تعریف می‌کند و اشاره می‌کند که این محدودیت بر اساس سه عنصر قرار گرفته است: پنهان کاری (کنترل اطلاعات)، ناشناسی (اقدام بدون توجه دیگران) و تنهایی (محدود کردن

ISSN: 2745-3673
http://www.Rcsj.ir

دسترسی فیزیکی به یک فرد). علاوه بر این، گیبس (۲۰۰۸) اشاره به اهمیت تعادل حریم خصوصی شخصی در برابر دیگر حقوق فردی و در برابر کالای اجتماعی جمعی دارد [۱۰].

چالش محرمانگی

محرمانگی اطلاعات بیانگر یک مسئله اساسی در اینترنت اشیا 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 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 اشیا، مربوط به قلمرو فیزیکی می‌باشد، 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 آنها می تواند به اعتبار و مزیت رقابتی شرکت ها در میان سایر شرکت ها آسیب وارد نماید. به عنوان مثال، می توان 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 به حوزه عمومی ممکن است باعث افزایش هرج و مرج و بروز وحشت و در معرض خطر قرار دادن امنیت گروه‌های زیادی از مردم شود.

در این زمینه تکنیک‌های 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 اشیا تناسب داشته باشد، ارائه گردیده است. این شیوه «کنترل دسترسی بر مبنای وظیفه» نام دارد. کنترل دسترسی بر مبنای وظیفه، به عنوان یک گزینه موفق که به طور گسترده و سطح بالایی برای کنترل دسترسی اختیاری و اجباری مورد استفاده قرار گرفته، در دو دهه گذشته ظهور یافته است.

در کنترل دسترسی بر مبنای وظیفه، دسترسی ها و کاربری ها به نقش ها اختصاص داده شده است. کاربران از طریق تعیین نقش، به طور غیر مستقیم مجوز لازم را کسب می کنند. در رویکرد اینترنت اشیا، مزیت عمده 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 اشیا، بیشتر نشان دهنده جریان اطلاعاتی است که در زمان واقعی در دسترس قرار می گیرند تا اینکه بیانگر یک پایگاه داده استاتیک باشد.

سیستم های مدیریت جریان داده به طور فزاینده ای برای حمایت از برنامه های کاربردی در زمان واقعی در یک گستره وسیع مورد استفاده قرار می گیرند (مانند نظارت بر شبکه، شبکه‌های حسگر و ...) و راه حل های مناسبی را برای اینترنت اشیا ارائه می دهند. در اینترنت اشیا، تکنیک های کنترل دسترسی باید با سیستم های مدیریت جریان داده ها ادغام شوند.

یکی از جنبه‌هایی که باید در زمان بروز مشکل محرمانه بودن در نظر گرفته شود، مدیریت شناسایی(هویت) است. در حقیقت این موضوع در فناوری اینترنت اشیا 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 حل‌ها به شیوه ای امن برای شناسایی اشیا و فرایندهای مربوط به صدور مجوز است [۹].

چالش اعتماد

یکی از چالش برانگیز ترین مشکلات فناوری اینترنت اشیا، 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 معیار می باشد. به عنوان تعریفی که به طور گسترده مورد استفاده قرار می گیرد، بیلز و فگیباوم، اعتماد را این گونه تعریف می کنند: اعتماد، سیاستهای امنیتی تنظیم شده 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 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 اشیا را پوشش دهد: ماهیت توزیعی سطح بالای اینترنت اشیا 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

ISSN: 2745-3673
http://www.Rcsj.ir

رابطه 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.

اگرچه ماهیت توزیعی و پویای اینترنت اشیا باعث می شود که موضوع اعتماد به شدت به چالش کشیده شود، ولی اینترنت اشیا به عنوان یک برنامه بسیار جالب از حیث مفاهیم اعتماد در نظر گرفته می شود. در حقیقت در زمینه ای که اشیا هوشمند خود به تصمیم گیری می پردازند، ابتدا باید رابطه اعتماد میان انسانها و اشیا پیرامون شان برقرار گردد. مهمترین و مرتبط ترین چالش های پژوهش در تعریف مکانیزم های مناسب اعتماد در اینترنت اشیا، عبارتند از:

- معرفی یک زبان ساده مذاکره در اعتماد که از نیازهای اینترنت اشیا در زمینه قابلیت همکاری حمایت نماید.
- تعریف یک مکانیزم مذاکره اعتماد بر پایه کنترل دسترسی مناسب به جریان اطلاعات.
- توسعه یک سیستم مدیریت مناسب برای شناسایی اشیا.
- طراحی یک چارچوب مدیریت اعتماد به طوری که منعطف و عمومی باشد و توانایی به کارگیری بخش‌های فوق الذکر را داشته باشد.

برنامه های کاربردی و خدمات در مقیاس اینترنت اشیا، در سرتاسر حوزه های اجرایی پیچیده، نیاز به یک چارچوب مطمئن برای توانایی کاربران سیستم ها به داشتن اعتماد دارد که بتوانند اطلاعات و خدمات قابل اتکاء را رد و بدل کنند [۹].

بحث و نتیجه‌گیری

توسعهٔ اینترنت همراه با اشیا و دستگاه‌های فیزیکی متصل به هم و نمایش مجازی آنها، روندی رو به رشد داشته است. به موجب این روند، دامنهٔ وسیعی از محصولات و خدمات جدید بالقوه در حوزه‌های مختلفی چون خانه‌های هوشمند، سلامت الکترونیکی، خودکارسازی، حمل و نقل و تدارکات و نظارت محیطی ایجاد شده است، مطالعات در این زمینه به تازگی اوج گرفته است و از طریق تلاش‌های مشترک دانشگاه‌ها، صنعت‌ها و مؤسسه‌های استاندارد در حوزه‌های مختلف، از جمله مخابرات و غیره پشتیبانی می‌شود. در حالی که سال‌های زیادی سیستم‌های قدیمی ابتدا برای مقاصد خاص با انعطاف‌پذیری محدود طراحی می‌شدند، اکنون ابتکار عمل در ساخت برنامه‌ها یا به طور کلی، اینترنت در آینده است که می‌تواند از اینترنت اشیا کاربردی و خدمات حوزهٔ اینترنت اشیا به جذب، ارتباط، ذخیره‌سازی، دسترسی و به اشتراک‌گذاری داده‌های دنیای فیزیکی اقدام کند. این کار فرصت‌های جدیدی در حوزه‌های گسترده‌ای مانند بهداشت الکترونیکی، خرده‌فروشی، انرژی سبز، تولید، شهر، سازمان، خانهٔ هوشمند و همچنین برنامهٔ کاربردی شخصی‌سازی شده کاربر نهایی، ایجاد کرده است.

تضمین امنیت سرویس‌ها و کاربردهای اینترنت، فاکتور بسیار مهمی در ایجاد اعتماد در کاربران و بکارگیری این بستر می‌باشد. کاربران باید اطمینان داشته باشند که اینترنت، کاربردهایش و تجهیزاتی که به آن متصل هستند، به اندازه کافی برای انجام فعالیت‌های آنلاین، در برابر تهدیداتی که وجود دارد، امن هستند. اینترنت اشیا نیز از این قاعده مستثنا نیست و امنیت این حوزه به اعتماد کاربران به محیط اطرافشان پیوند خورده است. اگر مردم به این اطمینان نرسند که تجهیزات و اطلاعاتشان بطور معقولی در برابر خرابی و سوء استفاده ایمن می‌باشند، این عدم اعتماد منجر به کاهش استفاده از کاربردهای مبتنی بر اینترنت اشیا خواهد شد. در واقع در سالیان گذشته تضمین امنیت در سرویس‌ها و محصولات اینترنت اشیا جزء اولویت‌های اول توسعه این حوزه بوده است و به شدت مورد توجه قرارگرفته است.

بحث امنیت امنیت شامل دسترسی غیرقانونی به اطلاعات و حمله هایی است که موجب قطعی فیزیکی در قابلیت دسترسی سرویس می گردد. در حالی که شهروندان دیجیتال با داده‌های موجود درباره مکان ها و فعالیت هایشان هرچه بیشتر ابزاری می‌گردند، به نظر می‌رسد که حریم خصوصی ناپدید می‌شود. سیستم های حفاظت از حریم خصوصی داده ها را جمع آوری می کنند و هنگامی که چالش های تکنولوژیکی با چالش های امنیتی مداوم دست به دست هم می دهند پاسخ های اورژانسی ارسال می‌کنند. این عمل برای یک شهر هوشمند که ما آرزوی زندگی در آن را داریم ضروری است. امنیت و حریم شخصی به طور گسترده ای از مسائل مهم در زمینه فناوری اینترنت اشیاء شناخته شده اند. از یک طرف، محرمانه بودن و یکپارچگی اطلاعات منتقل شده و ذخیره شده باید تضمین گردد، و احراز هویت و مکانیزم های صدور مجوز برای جلوگیری از دسترسی ناشایست کاربران و یا دستگاه های غیر مجاز نادرست فراهم گردد. از سوی دیگر، حریم خصوصی کاربران، به عنوان توانایی پشتیبانی از حفاظت داده ها و گمنام ماندن کاربران باید به عنوان یک جنبه اساسی به ویژه در ارائه اطلاعات حساس و یا شخصی در نظر گرفته شود.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[۱] فرازمند، عاطفه و احمدی، سروش،" اینترنت اشیاء و کاربردهای آن"، اولین همایش ملی کامپیوتر، فناوری اطلاعات و ارتباطات اسلامی، ۱۳۹۴.

[۲] بحرینی نژاد، اردشیر و همکاران، ۱۳۸۶، "راه حل برای اینترنت اشیاء"، دومین کنفرانس بین المللیRFID، تهران، ایران. ۱۳۸۶.

[۳] رهنورد. محمدیان. "سیستم مدیریت دانش جهت پوشش فرآیند خلق، سازماندهی، اشاعه و کاربرد دانش در خلق یک ارزش". ۱۳۸۸.

[۴] قاسمی. روح اله." حاکمیت اینترنت اشیاء: تجربیات کشورهای جهان و نقشه راه ایران". پژوهشگاه ارتباطات و فناوری اطلاعات. پژوهشکده سیاست گذاری و مدیریت راهبردی فاوا . گروه توسعه کسب و کار و کارآفرینی فاوا. ۱۳۹۴.

[۵] ارکیان. حمیدرضا و همکاران. "امنیت و حریم خصوصی در اینترنت اشیاء". دوفصلنامه علمی-ترویجی منادی امنیت فضای تولید و تبادل اطلاعات (افتا). دوره ۴. شماره ۲. ۱۳۹۴.

[۶] حسام‌تدین، محمد و همکاران. " شناسایی مراکز تحقیقاتی، چالشها و راه‌حل‌ها در امنیت اینترنت اشیا". وزارت ارتباطات و فناوری اطلاعات، مرکز تحقیقات مخابرات ایران، پژوهشکده امنیت ارتباطات و فناوری اطلاعات، گروه فناوری امنیت اطلاعات و سامانه‌ها. ۱۳۹۴.

[۷] فلاحی، فروغ. " بهینه سازی مصرف انرژی در ساختمان با استفاده از شبکه هوشمند حسگر بیسیم ، تابلوی مدیریت انرژی و کلیدهای هوشمند الکتریکی". اولین کنفرانس ملی ایده های نو در مهندسی برق. ۱۳۹۱.

[۸] مرکز ملی فضای مجازی. "اینترنت اشیا و کاربردهای فناری اینترنت اشیا". شواری عالی فضای مجازی ایران، مرکز ملی فضای مجازی. ۱۳۹۶.

[۹] لطفی. مجتبی. "امنیت اینترنت اشیا (IOT)". فروشگاه اینترنتی و تخصصی محصولات هوشمند سازی، اینترنت اشیا و آی تی. ۱۳۹۶.

[۱۰] پورشایسته، سیدعلیرضا و همکاران. "برسی امنیت در اینترنت اشیا با استفاده از راهکارهای تکنولوژی بلاک چین". هفتمین همایش سالانه بانکداری الکترونیک و نظام های پرداخت. تهران. ایران. مرکز همایش های بین المللی برج میلاد. بهمن ماه ۱۳۹۶.

[11] Parello, J.; Claise, B.; Schoening, B.; Quittek, J. "Energy Management Framework". IETF Internet Draft draft-ietf-eman-framework. (28 April 2014).

[12] Nasrin Mollanezhad Ashlaghi, Mohammad Heydari, Ehsan Ahadmotlaghi. The Study of the Effect of Internet Marketing Strategies on Development of the Export Market (Case Study: Pars Wagon Company), European Online Journal of Natural and Social Sciences; Vol.4, No.1. 2016.