اینترنت اشیاء : معماری و چالش‌ها

سینا قاضی‌نژاد [۱]، نرگس حبیبی* [۲]

۱- دانشجوی کارشناسی ارشد ، دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان) ، ایران

sinaghazinezhad@gmail.com

۲- استادیار، دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان) ، ایران

narges.habibi@gmail.com

چکیده

ظهور اینترنت اشیاء یکی از پدیده های قابل توجه در تاریخ محاسبات دیجیتال است. رشد سریع دستگاه‌های با قابلیت اتصال به اینترنت، از حسگرهای ساده تا سرورهای ابری پیچیده منجر به شکل گیری اینترنت اشیاء شد. الگویی مدرن که در آن اشیاء می‌توانند طیف وسیعی از موجودیت‌ها از قبیل لامپ‌های هوشمند، دوربین‌ها، لوازم خانگی، دستگاه‌های فروش، ترموستات و غیره را در برگیرند. شباهت تمامی این اشیاء توانایی اتصال به اینترنت و تبادل داده بدون دخالت انسان است. جهت ساخت سیستم‌های قابل اعتماد و برنامه‌های کاربردی مورد نیاز دراینترنت اشیاء نیاز حیاتی به یک معماری لایه بندی انعطاف پذیر وجود دارد. بسیاری از سازمان‌های بین‌المللی شناخته‌شده بر اساس نیازمندی‌های برنامه، توپولوژی شبکه، پروتکل‌ها، مدل‌های کسب و کار، خدمات و غیره چارچوب‌ها و معماری‌های مختلفی را ارائه نموده‌اند که ما دراین مقاله بر روی یک معماری امنیتی که توسط اتحادیه بین المللی مخابرات پیشنهاد شده است متمرکز شده‌ایم. همچنین در انتها طبقه‌بندی‌ای از چالش‌های موجود در اینترنت اشیاء طبق معماری ذکر شده مورد بررسی و کاوش قرار گرفته است.

کلمات کلیدی: اینترنت اشیاء، معماری اینترنت اشیاء، چالش‌ها در اینترنت اشیاء

۱– مقدمه

رشد بسیار سریع دستگاه‌های با قابلیت اتصال به اینترنت، از حسگرهای ساده تا سرورهای ابری پیچیده منجر به شکل-گیری اینترنت اشیاء[1] شد[۱]. اینترنت اشیاء شبکه‌ای از اجزاء فیزیکی(از قبیل ابزارهای پوشیدنی، لوازم برقی خانگی، سیستم‌های امنیتی، نانوتکنولوژی، ابزارهای ساخت و تولید و غیره) است. که به اجزاء هوشمندی (از قبیل ریزپردازنده‌ها، حافظه‌های ذخیره-سازی، سنسورها و غیره) مجهز شده‌اند و بر بستر اینترنت با سایر ابزارها ارتباط برقرار می‌کنند[۲]. قابلیت اتصال به شبکه امکان کنترل اشیاء از راه دور را با کمک زیرساخت‌های شبکه موجود که منجر به یکپارچه‌سازی با دنیای واقعی و بدون کمترین دخالت انسانی می‌شود را به ما می‌دهد. اشیاء از طریق تکنولوژی‌های زیربنایی از قبیل محاسبات فراگیر، قابلیت‌های ارتباطاتی، پروتوکل‌ها و اپلیکیشن‌ها از حالت کلاسیک و سنتی به هوشمند تبدیل می‌شوند. پروتوکل‌ها به منظور شناسایی زبان مورد استفاده در دستگاه‌های مختلف و همچنین ساختار و تبادل پیام‌ها به کار می‌روند[۱].

اینترنت اشیا با پوشش دادن عرصه‌های مختلفی از قبیل مراقبت پزشکی، اتومبیل‌ها، سرگرمی، لوازم صنعتی، ورزش، منازل و غیره نقش مهمی در تمامی جنبه‌های زندگی روزمره ما ایفا می‌کند. فراگیر شدن اینترنت اشیا باعث سهولت انجام فعالیت‌های روزمره و همچین غنی‌تر شدن ارتباطات افراد با محیط پیرامونشان و همچنین اشیاء مختلف خواهد شد. با این حال این دیدگاه همه منظوره باعث بروز نگرانی‌هایی در خصوص سطح امنیت و همچنین حریم خصوصی کاربران خواهد شد[۳] که در بخش چالش‌ها بدان خواهیم پرداخت.

---

[1] Internet of things

۲- جنبه‌های تاریخی

اولین بار مفهوم اتصال بین دستگاه‌های هوشمند در اوایل دهه ۱۹۸۰ زمانی مطرح شد که یک ماشین فروش خودکار اصلاح‌شده۲ در دانشگاه کارنگی‌ملون با قابلیت اتصال به اینترنت قادر بود تا فهرست نوشیدنی‌های موجود را بررسی و گزارش کند. در سال ۱۹۹۱، دیدگاه کنونی اینترنت اشیاء توسط مارک وایزر در مقاله خود در مورد محاسبات فراگیر رایانه قرن ۲۱ ارائه شد[۴, ۵]. در سال ۱۹۹۹ بیل جویی سرنخ‌هایی را در زمینه‌ی ارتباطات ماشین به ماشین در طبقه‌بندی خود در زمینه اینترنت ارائه نمود[۴]. واژه IOT اولین بار در سال ۱۹۹۹ در یک سخنرانی توسط کوین اشتون که یکی از بنیانگذاران مرکز شناسایی خودکار در موسسه فن‌آوری ماساچوست است معرفی شد[۶]. اشتون IOT را به شکل سیستمی ارتباطی بین دنیای فیزیکی و اینترنت از طریق به کارگیری فناوری شناسایی امواج رادیویی۳ و دستگاه‌های حسگر که قابلیت نظارت بر محیط اطراف و شناسایی در دنیای واقعی را دارند توصیف نمود[۶]. در سال ۲۰۰۵ با انتشار نخستین گزارش از سوی اتحادیه بین المللی مخابرات در رابطه با مفهوم اینترنت اشیاء، این اصطلاح به طور گسترده و رسمی مورد استفاده محققین و صنعت‌گران قرار گرفت[۷].

۳- معماری اینترنت اشیاء

اینترنت اشیاء باید قادر به اتصال میلیاردها اشیاء ناهمگن از طریق اینترنت باشد، از آنجایی‌که اینترنت اشیاء در زمینه‌های مختلف کاربردی نظیر مراقبت های بهداشتی، سیستم های حمل و نقل هوشمند و مدیریت صنعتی کاربرد دارد، به این ترتیب، تحقق مسائل امنیتی به منظور ایجاد سیستم‌های قابل اعتماد و برنامه‌های کاربردی مورد نیاز است. بنابراین نیاز حیاتی برای یک معماری لایه بندی انعطاف پذیر وجود دارد[۶]. معماری اینترنت اشیاء باید به اندازه کافی انعطاف پذیر باشد تا بتواند پاسخگوی عوامل مختلفی از قبیل کیفیت سرویس، مدولار بودن۴، قابلیت اطمینان، مدیریت حریم خصوصی، تعامل معنایی۵، پشتیبانی دستگاه‌های مختلف و غیره باشد[۵]. بسیاری از سازمان‌های بین‌المللی شناخته‌شده و گروه‌های کاری از قبیل اتحادیه بین المللی مخابرات۶، انجمن مهندسان برق و الکترونیک۷، سازمان سیسکو، موسسه استانداردسازی ارتباطات اروپا۸ بر اساس نیازمندی‌های برنامه، توپولوژی شبکه، پروتکل‌ها، مدل‌های کسب و کار، خدمات و غیره چارچوب‌هایی را ارائه کرده اند. با این حال، هیچ یک از آنها تا به این تاریخ استاندارد نشده است [۵, ۶].

در این بخش، یک معماری امنیتی که توسط اتحادیه بین المللی مخابرات پیشنهاد شده است مورد بررسی قرار گرفته است. با توجه به این معماری، اینترنت اشیا را می توان به ۳ لایه تقسیم کرد: لایه ادراک، انتقال و کاربرد. هرکدام ازین لایه‌ها می توانند به زیر لایه‌هایی تقسیم شوند که در جلوتر بررسی خواهیم نمود. این معماری پیشنهادی در شکل ۱ قابل مشاهده است[۸, ۹].

---

[2] Coke machine
[3] Radio-frequency identification
[4] Modularity
[5] Semantic interoperability
[6] International Telecommunication Union
[7] Institute of Electrical and Electronics Engineers (IEEE)
[8] European Telecommunications Standards Institute (ETSI)

لایه‌های اصلی	زیرلایه‌ها	ویژگی‌های کلیدی	تکنولوژی‌های کلیدی
لایه کاربرد	برنامه‌های اینترنت اشیاء	ترمینال‌ها، واسط‌های کاربری، تلفن‌های همراه و تبلت‌ها	رایانش ابری، میان‌افزارها و ارتباطات ماشین به ماشین
لایه انتقال	شبکه محلی و گسترده	ایجاد اتصال و انتقال اطلاعات	اینترنت، وای‌فای و شبکه-های ادهاک
	شبکه هسته		
	شبکه دسترسی		
لایه ادراک	شبکه ادراک	سنجش، هویت‌یابی و تکنولوژی‌های ارتباطی	بلوتوث، سیستم شناسایی امواج رادیویی و شبکه‌های حسگر بی‌سیم
	گره‌های ادراک		

شکل ۱ : معماری ۳ لایه پیشنهادی توسط توسط اتحادیه بین المللی مخابرات برای اینترنت اشیاء

۳-۱ : لایه ادراک [9]:

این لایه شامل تکنولوژی‌هایی به منظور سنجش[10](جمع‌آوری داده‌ها از محیط اطراف و ارسال آن به پایگاه داده، انبار داده یا سرویس ابری) .هویت‌یابی[11](شناسایی اشیاء بر اساس شناسه منحصر به فردی که به آن ها تخصیص داده شده است) و ارتباطات (برقراری ارتباط بین دستگاه‌های هوشمند ناهمگن) با حداقل دخالت انسانی است. این لایه همچنین می‌تواند به دو زیرلایه گره‌های ادراک[12] و شبکه ادراک[13] تقسیم شود[۴, ۵].

۳-۱-۱ : گره‌های ادراک

منظور از گره های ادراک دستگاه های فیزیکی یا اشیائی از قبیل حسگرها، عملگرها۱۴ ، کنترلرها و غیره می باشند. این دستگاه‌های فیزیکی می توانند سیستم‌های بارکدخوان، سامانه‌های شناسایی امواج رادیویی، بلوتوث و حسگرهای مختلف باشندکه هدف آن‌ها جمع آوری اطلاعات از محیط پیرامون، شنایی اشیاء، کنترل داده و کنترل اشیا می‌باشد. بسته به ماهیت دستگاه‌های استفاده شده، اطلاعات جمع آوری شده می تواند به خواص شیء از قبیل محل قرارگیری، دما، میزان رطوبت و سایر شرایط محیطی مرتبط باشد[۵].

۳-۱-۲ : شبکه ادراک

این شبکه که مسئول ارتباط با لایه انتقال است، وظیفه دارد داده‌های جمع آوری شده توسط گره‌های ادراک را به شیوه‌ای امن به دروازه‌ها۱۵ منتقل کند و سیگنال‌های کنترل را به دستگاه های کنترلی از طریق رسانه های ارتباطی سیمی یا بی سیم ارسال می‌کند[۸].

---

[9] Perception layer
[10] Sensing
[11] Identification
[12] Perception nodes
[13] Perception network
[14] Actuator
[15] Gateway

۳-۲ : لایه انتقال[16]

این لایه که تحت عنوان لایه حمل و نقل یا لایه شبکه نیز شناخته می شود به عنوان یک لایه میانجی بین لایه ادراک و کاربرد قرار گرفته است[۸]. این لایه می‌تواند شبکه‌های ناهمگن مختلف، تکنولوژی‌ها و پروتوکل‌ها را با هم یکپارچه کند و هدف آن انتقال داده‌های جمع آوری شده توسط گره‌های ادراک به واحد پردازش اطلاعات جهت تحلیل، اکتشاف داده، یکپارچه‌سازی و رمزگذاری داده است. این لایه همچنین مسئولیت ارائه عملکردهای مختلف جهت مدیریت شبکه را نیز عهده‌دار می‌باشد. این لایه می‌تواند به سه زیر لایه شبکه دسترسی۱۷، شبکه هسته۱۸ و شبکه محلی و گسترده۱۹ تقسیم بندی شود[۵].

۳-۲-۱ : شبکه دسترسی

این لایه به عنوان نوعی شبکه مخابراتی علاوه بر فراهم نمودن یک دسترسی گسترده به لایه ادراک، به عنوان پلی بین مشترکین و ارائه دهندگان خدمات نیز عمل می‌کند. این شبکه ارتباطات و قابلیت‌های زیر بنایی از قبیل ارتباطات تلفن همراه، ارتباطات ماهواره‌ای و ارتباطات بی‌سیم را برای کاربران نهایی فراهم می‌کند. شبکه دسترسی‌ای که اینترنت اشیاء می‌تواند پیاده سازی کند شبکه‌های ادهاک، وای فای، زیگ‌بی۲۰، بلوتوث، شبکه‌های نسل چهارم و پنجم۲۱ و غیره هستند. بسته به وجود یک مرکز سنترال، لایه دسترسی می‌تواند متمرکز (مانند وای‌فای) یا غیر متمرکز (مانند شبکه‌های ادهاک) باشد [۵, ۹].

۳-۲-۲ : شبکه هسته

شبکه هسته ، اینترنتی است که چارچوب اصلی را برای اینترنت اشیاء فراهم می کند و همچنین مسئول انتقال داده به کابران نهایی که به شبکه متصل شده‌اند را دارا می‌باشد. شبکه هسته بخش مرکزی هر شبکه مخابراتی است و به عنوان ستون فقرات برای تبادل اطلاعات و خدمات عمل می کند. این لایه ارتباطات را در میان دستگاه‌ها برای به اشتراک گذاری منابع ایجاد می کند. اینترنت را می توان به عنوان شبکه عمومی، خصوصی و یا کسب و کار مورد استفاده قرار داد و می‌تواند گستره محلی و همچنین وسیعی را پوشش دهد. این لایه همچنین قابلیت مشاهده و کنترل اشیاء فیزیکی از راه دور را فراهم می‌کند[۹].

۳-۲-۳ : شبکه محلی و گسترده

شبکه محلی اتصال بین دستگاه‌ها در یک منطقه نسبتا کوچک است. دستگاه‌ها در یک شبکه محلی می‌توانند به طور مستقیم بین خودشان ارتباط برقرار کنند و همچنین می‌توانند با دستگاه‌های از راه دور از طریق دروازه ارتباط برقرار کنند. به شکل مشابه شبکه‌های گسترده به عنوان توزیعی از دستگاه‌ها در یک منطقه جغرافیایی بزرگ در نظر گرفته می شوند. شبکه های گسترده با توان پایین۲۲ مورد توجه بیشتری قرار دارند چرا که این شبکه‌ها از اتصال دستگاه‌های با توان محدود نیز پشتیبانی می‌کنند[۹].

۳-۳ : لایه کاربرد[23]

هدف لایه کاربرد که برای کاربر نهایی قابل مشاهده است مدیریت و ارائه برنامه‌های کاربردی براساس اطلاعات جمع‌آوری‌شده توسط لایه ادراک است. این لایه دسترسی به سرویس‌های شخصی برای کاربران نهایی را بر روی شبکه با توجه به نیازهای آن‌ها از طریق دستگاه‌های مختلف و تجهیزات ترمینال فراهم می‌کند[۵, ۹]. به عنوان مثال این لایه می‌تواند

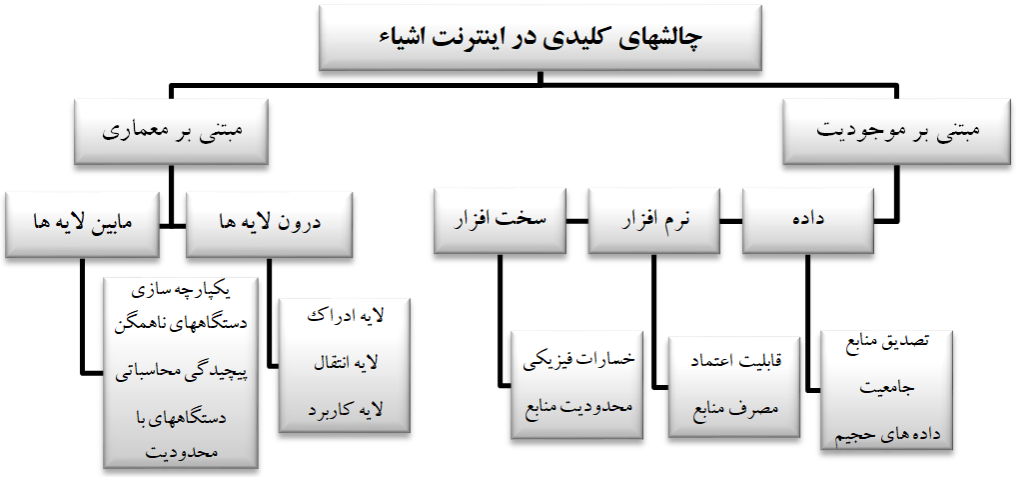
---

[16] Transmission layer
[17] Access Network
[18] Core Network
[19] Local and Wide Area Network
[20] ZigBee
[21] 4G-LTE and 5G
[22] Low Power Wide Area Networks
[23] Application layer

میزان دما و رطوبت اندازه گیری شده توسط حسگرها را در قبال درخواست کاربران برای آن‌ها فراهم کند. اهمیت این لایه در اینترنت اشیاء بدان جهت است که قابلیت ارائه خدمات هوشمند با کیفیت بالا در جهت برآورده کردن نیازهای مشتریان را دارد[۱۰].

۴- چالش‌ها در اینترنت اشیاء

اینترنت اشیاء الگویی جدید و مدرن با پتانسیل بالاست که می‌تواند شکل معمول استفاده از اینترنت را تغییر دهد. با این وجود اینترنت اشیاء با تمام قابلیت‌هایی که دارد چالش‌های زیادی را در لایه‌های مختلف معماری پیش پای ما می‌گذارد. شکل ۲ چالش‌های مبتنی بر معماری و چالش‌های مبتنی بر موجودیت را نشان می‌دهد. چالش‌های مبتنی بر معماری، مسایل خاص مربوط به هر لایه و نیز مسایل مربوط به یکپارچه‌سازی لایه‌ها در یک چارچوب واحد را پوشش می‌دهند. چالش‌های بر پایه موجودیت بر مسائل در ارتباط با اجزای سه نهاد اساسی هر سیستم محاسباتی یعنی سخت‌افزار، نرم‌افزار و داده‌ها تمرکز دارد[۵].



۴–۱ : چالش‌های مرتبط با معماری

۴–۱–۱ : چالش‌های ما بین لایه‌ها

لایه های تعریف شده در معماری با مقدار زیادی ناهمگونی همراه است که متقابلا موجب ایجاد مسائل یکپارچه سازی ناهمگن بین لایه‌ها می‌شود. کاربران می‌توانند به داده های جمع آوری شده از محیط (که توسط گره های ادراک از لایه انتقال عبور می کنند) از طریق برنامه‌های کاربردی دسترسی داشته باشند. داده‌ها می‌توانند به روش‌های مختلف، در فرمت‌های مختلف، با استفاده از پروتکل‌های مختلف و برای اهداف مختلف جمع‌آوری شوند. بنابراین، استانداردسازی داده‌ها در هر لایه ضروری است. اگر از تکنولوژی یکپارچه‌سازی درستی اطمینان حاصل نشود ممکن است منجر به تخریب داده‌ها شود و یا اینکه داده‌ها ، داده‌های مورد اعتمادی نباشند. علاوه بر این، هر لایه مکانیسم های مختلفی برای اطمینان از امنیت، حریم خصوصی و اعتبار اطلاعات نیاز دارد. از این رو، پیچیدگی محاسباتی به واسطه مکانیزم های مختلفی که در هر لایه اعمال می شود، به وجود می‌آید. بنابراین بهینه‌سازی بین لایه‌ها، به ویژه زمانی که تعداد زیادی از دستگاه‌های ناهمگن از طریق اینترنت به هم متصل می‌شوند، موردنیاز می‌شود[۱۰]. دستگاه‌هایی که برای انجام کارکردها در هر لایه بکار گرفته می‌شوند، نیاز به منابع متفاوتی دارند. به عنوان مثال، ممکن است دستگاه هایی با محدودیت منابع وجود داشته باشند مانند سنسور درجه حرارت که

داده‌هایی را از محیط اطراف(با حجم چند کیلوبایت) خوانده و ثبت می‌کند. در حالی که ممکن است سرورهای رده بالایی وجود داشته باشند که داده‌ها را از سنسورهای دمایی مختلف جمع آوری کرده و پس از پردازش داده‌های انبوهی را تولید کنند[۹].

۴-۱-۲: چالش‌های درون لایه‌ها

گره‌های ادراک قرار است در شرایط محیطی متنوع مستقر شوند و مستعد خسارات فیزیکی هستند. به عنوان مثال سنسورهایی برای نظارت بر رشد گیاهان ممکن است در زیر خاک مستقر شوند یا سنسورهایی برای نظارت بر فعالیتهای جزر و مدی در آب دریا غوطه‌ور شوند. علاوه بر این، گره‌ها به حملاتی مانند تکذیب سرویس[۲۴] و سایر اقدامات مخرب که می‌توانند پارامترهای عملیاتی را دستکاری کنند، آسیب پذیر هستند. بنابراین، اطمینان از اینکه هیچ فعالیت مخرب یا رویداد فیزیکی کارهای عادی گره‌ها را مختل نمی‌کند، ضروری است. اطمینان از احراز هویت گره‌ها و یکپارچگی داده ها از دیگر مسائل کلیدی هستند[۵, ۱۱].

در این لایه، تراکم شبکه[۲۵] و شناسایی منحصر به فرد دستگاه‌ها به چالش‌های موجود می‌افزاید. این لایه همچنین مستعد حملاتی مانند تکذیب سرویس، فیشینگ[۲۶]، نفوذ بدافزار، حملات دسترسی[۲۷]، افشا اطلاعات[۲۸] و غیره است[۱۲].

از آنجایی که لایه کاربرد با برنامه های کاربردی متعدد مرتبط با کسب و کار یا فردی ارتباط دارد، با مسائل کلی و امنیتی تمام این برنامه‌ها مانند وقفه سرویس[۲۹]، افشای اطلاعات، و حریم خصوصی پرس و جو[۳۰] همراه است. همچنین دستگاه‌های هوشمند که از دسترسی به انواع برنامه‌های کاربردی پشتیبانی می‌کنند دارای ظرفیت باتری و ظرفیت ذخیره‌سازی محدودی هستند. و همچنین توانایی محاسباتی محدودی دارند[۱۲].

٤-۲ : چالش‌های مرتبط با موجودیت‌ها

۴-۲-۱ : سخت افزار

لازم است برای محافظت از دستگاه های سخت افزاری، از جمله دستگاه‌های ذخیره سازی اطلاعات حجیم و سرورهایی که نرم‌افزارها در آنها مستقر شده است و برنامه‌های کاربردی روی آن‌ها در حال اجراست از آسیب‌های فیزیکی جلوگیری شود. این خسارات فیزیکی ممکن است به علت بلایای طبیعی و همچنین اقدامات مخرب عمدی توسط مهاجمان رخ دهد. ایمنی اتصالات ارتباطات سیمی نیز ضروری است زیرا مسئول حمل داده‌ها از تعداد زیادی گره حسگر هستند و همچنین ممکن است قطع یا بریده شوند. همچنین، قابلیت‌های یکپارچه‌سازی بر روی دستگاه‌های سخت افزاری که محدودیت منابع دارند، چالش برانگیز است[۱۳].

۴-۲-۲ : نرم‌افزار

نرم افزارها ممکن است برنامه‌های ارتباطی، برنامه‌های کاربردی امنیتی یا نرم‌افزار سیستمی مانند سیستم عامل یا نرم‌افزارهای مدیریت پایگاه داده برای توسعه و اجرای نرم افزار کاربردی باشند. هر مهاجم می‌تواند کار عادی نرم افزار را مختل کند که ممکن است باعث بحرانی بزرگ شود[۳]. نرم افزار کاربردی قابل دسترس برای کاربران نیز دارای درجه بالایی از آسیب پذیری است. سطوح پیچیدگی متفاوتی در میان نرم افزارهای مورد نیاز برای وظایف شامل سنجش اطلاعات، پردازش، مدیریت، ایجاد امنیت و غیره وجود دارد. با افزایش اندازه نرم افزار، مصرف منابع و هزینه کلی سیستم نیز افزایش می یابد. توسعه

[24] Denial of Service
[25] Network congestion
[26] Phishing
[27] Access attacks
[28] Information disclosure
[29] Service interruption
[30] Query privacy

راه‌حل‌های کم هزینه و با مصرف انرژی پایین برای دستگاه‌های دارای محدودیت و توسعه یک اکوسیستم نرم افزاری که بتواند نیازمندی‌های مختلف را برآورده کند نیاز به تفکر جدیدی در طراحی و تصمیم گیری‌های مهندسی صحیح دارد[۳, ۹].

۴-۲-۳ : داده

داده‌ها دارایی اولیه کاربر در محیط دیجیتال هستند و هدف هر سیستم محاسباتی سر و کار داشتن با داده‌هاست. بنابراین، پایگاه‌های‌داده‌ها نیز نیاز به حفاظت دارند. داده ها ممکن است به یک فرد، یک گروه یا یک سازمان تعلق داشته باشند و سطح حساسیت محتوا نیز با توجه به استفاده متفاوت است. به عنوان مثال، رکوردهای مربوط به سوابق درمانی یک فرد حساسیت بیشتری نسبت به داده‌های دمایی خوانده شده توسط یک سنسور دارد[۱۴]. داده‌ها ممکن است مورد دسترسی، اصلاح و تخریب غیر مجاز قرار گیرند. با توجه به تعدد دستگاه‌های موجود در اینترنت اشیاء، تایید اعتبار داده‌ها و منبع آن دشوار است. داده های مخرب را می‌توان از طریق کانال‌های ارتباطی به شبکه منتقل کرد. بنابر این توسعه طرح‌های سبک‌وزن مبتنی بر رمزنگاری، امضای دیجیتالی، رمزگذاری هش و غیره برای حفاظت از داده‌ها برای تضمین قابلیت اعتماد و انسجام در یک محیط ناهمگن با دستگاه های دارای محدودیت منابع یک چالش بزرگ دیگر است. علاوه بر این، داده‌های تولید شده توسط دستگاه‌ها به صورت عمده، به عنوان کلان داده، نیاز به تکنیک‌های مدیریت داده سبک وزن دارد[۱۵].

۵- نتیجه‌گیری

اینترنت اشیاء چشم اندازی رو به پیشرفت است. ایده‌ی جذابی که در آن هر شیء و هر دستگاهی دارای هویت دیجیتال و قابلیت اتصال به اینترنت و تبادل داده خواهد بود. ماهیت پویای اینترنت اشیاء، همچنین مقیاس پذیری و وجود دستگاه‌های متعدد ناهمگن چالش‌های بزرگی را پیش روی ما خواهند گذاشت. چالش‌هایی که می‌توان آن‌ها را در زمینه‌های حریم خصوصی، امنیت، مدیریت و تجزیه تحلیل داده و غیره طبقه بندی نمود. که در مقاله به معرفی و تشریح برخی ازین چالش‌ها پرداخته شد. همچنین یک معماری چندلایه پیشنهادی توسط اتحادیه بین المللی مخابرات با تاکید بر مسائل امنیتی
مورد کاوش و بررسی قرار گرفت.

مراجع

[1] MahmoudAmmar, GiovanniRussello, and BrunoCrispoa, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, vol. 38, pp. 8-27, 2018.

[2] A. Paul and R. Jeyaraj, "Internet of Things: A primer," Human Behaviour and Emerging Technology, vol. 1, no. 1, pp. 37-47, 2019.

[3] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, pp. 2787-2805, 2010.

[4] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A Review on Internet of Things (IoT)," International Journal of Computer Applications, vol. 113, pp. 1-7, 2015.

[5] B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," Concurrency and Computation: Practice and Experience, pp. 291-319, 2018.

[6] P. P. Ray, "A survey on Internet of Things architectures," Journal of King Saud University - Computer and Information Sciences, vol. 30, no. 3, pp. 291-319, 2018.

[7] EleonoraBorgia, "The Internet of Things vision: Key features, applications and open issues," Computer Communications, vol. 54, pp. 1-31, 2014.

[8] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things," presented at the 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), Chengdu, China, 2010.

[9] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

[10] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17 no. 4, pp. 2347 - 2376, 2015.

[11] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems vol. 29, no. 7, pp. 1645-1660, 2013.

[12] P. I. R. Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the Internet of Things: Challenges, threats and solutions," Internet of Things, vol. 5, pp. 41-70, 2019.

[13] R. Fantacci, T. Pecorella, R. Viti, and C. Carlini, "A network architecture solution for efficient IOT WSN backhauling: challenges and opportunities," IEEE Wireless Communications, vol. 21, no. 4, pp. 113 - 119, 2014.

[14] J. E. Siegel, S. Kumar, and S. E. Sarma, "The Future Internet of Things: Secure, Efficient, and Model-Based," The Future Internet of Things: Secure, Efficient, and Model-Based, vol. 5, no. 4, pp. 2386-2398, 2018.

[15] S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497-1516, 2012.