مجله نخبگان علوم و مهندسی
Journal of Science and Engineering Elites
جلد ۸- شماره ۳ - سال ۱۴۰۲
www.ElitesJournal.ir

بررسی ساختار و پروتکل های اینترنت اشیاء

مهدی بردبار*[۱]، محمد رحمانی[۲]، آرمین زاکاریان[۳]

۱- دانشجوی دکتری کامپیوتر- نرم افزار،دانشگاه آزاد اسلامی واحد مشهد
۲- دکتری تخصصی مهندسی فناوری اطلاعات،دانشگاه تهران
۳- دکتری تخصصی مهندسی فناوری اطلاعات،دانشگاه تهران

* emehdibordbar@gmail.com

ارسال: مرداد ماه ۱۴۰۲ پذیرش: مرداد ماه ۱۴۰۲

چکیده

امروزه اینترنت اشیا (IOT) به مفهومی جدید مبدل شده و تأثیرات بسیار بزرگی روی دنیا گذاشته است. به‌طور قطع هرچقدر اینترنت اشیاء رشد بیشتری پیدا کند، به همان اندازه نیز کاربردهای آن بیشتر خواهد شد. با توجه به اینکه اینترنت اشیاء روشی عالی برای هوشمندسازی جهان است، به‌طور قطع در آینده نیز با رشد بیشتری همراه خواهد شد. اینترنت اشیاء به عنوان الگویی تعریف می گردد که در آن اشیاء مجهز به حس گرها، محرک ها و پردازش گرها با یکدیگر ارتباط برقرار می کنند تا هدف معناداری را دنبال کنند. پروتکل‌های اینترنت اشیا بخشی جدایی ناپذیر از معماری آن هستند. بدون پروتکل‌ها و استانداردهای اینترنت اشیا، سخت افزار بی فایده تلقی می‌شود زیرا به دلیل وجد آن‌ها، تبادل داده توسط سخت افزار امکان‌پذیر می گردد و از بین این داده‌های منتقل شده، اطلاعات مفید می‌تواند توسط کاربر نهایی استخراج شود.مقاله حاضر در مقایسه با مقالات تحقیقاتی در این زمینه، دارای پوشش جامع تر بوده و به طور گسترده دامنه فناوری های عمده از جمله ساختار و پروتکل ها را بررسی می کند.

کلمات کلیدی: اینترنت اشیاء،پروتکل،معماری اینترنت اشیاء.

۱- مقدمه

امروزه اینترنت به مسئله ای فراگیر تبدیل شده و تقریبا هر گوشه از کره جهان را تحت پوشش قرار داده است و به شیوه های غیرقابل تصور بر زندگی انسان تاثیر می گذارد. به هر حال، این روند هنوز ادامه دارد. حال وارد عصر اتصال جامع می شویم که در آن انواع گسترده وسایل به وب وصل می شوند. ما وارد عصر «اینترنت اشیا» می شویم. مولفین به شیوه های مختلفی به تعریف این مسئله پرداخته اند. حال نگاهی به دو تعریف معروف می اندازیم. ورمیزن با همکاران اینترنت اشیا را صرفا تعامل بین جهان فیزیکی و دیجیتال تعریف می کنند. جهان دیجیتال از طریق حس گرها و محرک های بی شماری با جهان فیزیکی تعامل برقرار می کند. تعریف دیگر پنا-لوپز با همکاران می باشد که اینترنت اشیاء را به عنوان الگویی تعریف می کنند که در آن محاسبه و شبکه بندی قابلیت ها در هر نوع شی امکان پذیر نهفته شده است. از این توانمندی ها برای جستجوی وضعیت شی و تغییر وضعیت آن در صورت ممکن استفاده می کنیم. به بیان ساده تر، اینترنت اشیاء اشاره به نوع تازه ای از جهان دارد که در آن تقریبا تمامی ابزارها و وسایل که استفاده می کنیم به شبکه ای متصل هستند. می توانیم از انها به طور مشترک استفاده کنیم تا فعالیت های پیچیده ای را انجام دهیم که نیاز به درجه هوش بالایی دارند .ابزارهای اینترنت اشیاء به منظور این هوش و ارتباط مابین مجهز به حسگرها، محرک ها، پردازش گرها و فرستنده های نهفته اند. اینترنت اشیاء نوعی فناوری واحد نیست، بلکه مجموعه ای از فناوری های متنوع است که با همدیگر

کار می کنند.حس گرها و محرک ها ابزارهایی اند که به تعامل با محیط فیزیکی کمک می کنند. داده های جمع آوری شده با حس گرها بایستی به طور هوشمندانه ذخیره و پردازش شوند به منظور اینکه بتوان مطالب مفیدی را از آنها استنباط نمود. دقت کنید که به طور جامع به تعریف واژه حس گر می پردازیم؛ تلفن همراه یا حتی ماکروفر که می تواند به عنوان حس گر عمل کند تا زمانی که مطالب ورودی درباره وضعیت فعلی خود (وضعیت داخلی+ محیط) فراهم می کند. محرک ابزاری است که برای اثرگذاری بر تغییر در محیط از جمله کنترل گر دمای کولر گازی به کار می رود .ذخیره و پردازش داده ها را می توان در خود شبکه یا سرور از راه دور انجام داد. اگر هر نوع پیش پردازش داده ها ممکن باشد، آن از طریق حس گر یا ابزار مجاور صورت می گیرد. سپس داده های پردازش شده به سرور از راه دور ارسال می گردد. قابلیت های ذخیره و پردازش اینترنت اشیاء محدود به منابع موجود است که محدودیت اندازه، انرژی، قدرت و قابلیت محاسبه دارند. در نتیجه، چالش تحقیقاتی عمده اطمینان از آن است که به نوع صحیح داده ها در سطح مطلوب دقت دست یابیم. در امتداد چالش های جمع آوری داده ها و کنترل آن، چالش هایی در ارتباطات نیز وجود دارد. ارتباطات بین ابزارهای اینترنت اشیاء به طور عمده بی سیم است چون آنها در کل در نواحی جغرافیایی پراکنده نصب می شوند. کانال های بی سیم اغلب میزان انحراف بیشتری دارند و غیر قابل اعتماد اند .دراین منظر، انتقال داده ها به طور معتبر بدون نیاز به انتقال مجدد مسئله مهمی است و لذا فناوری های ارتباطات بخش اساسی ابزارهای اینترنت اشیا می باشد.امروزه پس از پردازش داده های دریافتی باید برخی اقداماتی راجع به مبانی استنباط های دریافتی در پیش گرفت. ماهیت اقدامات ممکن است متنوع باشد. می توانیم به طور مستقیم جهان فیزیکی را از طریق محرک ها تعدیل کنیم.یا اینکه ممکن است کاری را به طور مجازی انجام دهیم. برای نمونه، می توانیم برخی اطلاعات به دیگر اشیا هوشمند ارسال کنیم.

۲- پیشینه پژوهش

اینترنت اشیاء شامل طیف گسترده‌ای از فناوری‌ها و تکنولوژی‌ها می‌باشد، بنابراین، مشکلات و چالش‌های موجود در هرکدام از این فناوری‌ها و تکنولوژی‌ها می‌تواند در بدنه اینترنت اشیاء نفوذ کند در زمینه چالش مربوط به تکنولوژی تحقیقات متعددی انجام شده است و این چالش در قالب دسته‌های مربوط به چالش معماری و طراحی نحوه آدرس‌دهی یکتا ناهمگونی دستگاه‌ها مدیریت اطلاعات ساختار سخت‌افزاری و تحمل خطا مطرح می‌شود. در تحقیق دیگری، ارتباط اینترنتی ضعیف به‌عنوان مهم‌ترین چالش تکنولوژی در مبحث اینترنت اشیاء معرفی شده است(کانتی و همکاران، ۲۰۱۸).

یکی از چالش‌های مطرح در بحث پیاده‌سازی اینترنت اشیاء، چالش امنیت است .این چالش در قالب مفاهیمی مانند احراز هویت کنترل دسترسی حریم خصوصی، معماری و ساختار امن تقسیم‌بندی می‌شود، با توجه به مقیاس وسیع بستر اینترنت اشیاء چالش امنیت و حریم خصوصی در مقایسه با سایر چالش‌های اینترنت اشیاء، مهم‌تر است. برای اینکه بستر اینترنت اشیاء با موفقیت راه‌اندازی شود باید نقش امنیت و حریم خصوصی به‌صورت جدی موردتوجه قرار گیرد. وقتی میلیاردها شیء به هم متصل می‌شوند برای حفاظت از اطلاعات، اشتراک‌گذاری داده‌ها بر روی رسانه انتقال اینترنت اشیاء و حفظ حریم خصوصی افراد، به مکانیزم های امنیتی دقیق نیاز است (رهسپارفرد و مولایی، ۱۳۹۷).

برخی از نمونه های مهم تر از برنامه های اینترنت اشیا در حوزه های زیر دسته بندی می‌شوند.:

۱- حوزه شخصی و اجتماعی شرکتها و صنایع نظارت بر خدمات و ابزار، و تحرک و حمل و نقل. حوزه شخصی و اجتماعی برنامه های کاربردی در این دسته به کاربران اجازه می دهند. تا با محیط اطراف خود (خانه و محل کار یا با افراد دیگر برای حفظ و ایجاد روابط اجتماعی تعامل داشته باشند.

۲ - حوزه تحرک و حمل و نقل وسایل نقلیه و حتی جاده ها با پردازنده های قدرت محرک ها و حسگرها، .با جمع آوری داده های مهم در مورد کنترل و راهنمایی ترافیک برای ارائه اطلاعات حمل و نقل مناسب ابزاری هستند.

۳ - حوزه بنگاهها و صنایع فعالیتها شامل معاملات مالی یا تجاری بین شرکتها، صنایع سازمانها و سایر نهادها از جمله تولیدی، لجستیکی، بخشهای خدماتی، بانکی مقامات مالی دولتی واسطه ها و غیره می شود.

۴ - حوزه نظارت بر خدمات و تاسیسات. این حوزه معمولاً با حفاظت نظارت و توسعه همه منابع طبیعی از کشاورزی و اصلاح نژاد گرفته. تا بازیافت خدمات مدیریت زیست محیطی مدیریت انرژی و غیره سروکار دارد (جهانگشته و همکاران،۱۴۰۱).

۳- اجزای ساختار اینترنت اشیاء

اینترنت اشیاء (IoT)[1] در حال تغییر طرز کار دنیای ما است؛ از خانه های هوشمند و پوشیدنی ها گرفته تا خرده فروشی و بانکداری. همه چیز از طریق گوشی های هوشمند ما قابل دسترسی است و تمامی وسایلمان به اینترنت متصلند. این یک سرمایه گذاری مطلوب است که اساساً با توجه به تغییرات مداوم نیاز مشتریان دچار تحول می شود. در این مقاله ۴ جنبه کلیدی یک شبکه IoT ارایه شده که به شما کمک می کند نیازهای تجاری خود را برآورده ساخته و خود را با این فناوری به روز کنید. در مطالعه انجام گرفته توسط شرکت سیسکو، پیش بینی می شود در آینده ای نزدیک تعداد ۵۰ میلیارد دستگاه متصل به اینترنت خواهیم داشت. امروزه، تقریباً ۲۰ میلیارد شیء یا چیز فیزیکی متصل به اینترنت وجود دارند که در داخل آنها حسگرهای گوناگون تعبیه شده، و دارای ارتباط نرم افزاری و شبکه هستند. این روند در حال تغییر دادن روش های کسب و کار و تکامل و ایجاد انقلاب در ساختار بالا به پایین کسب و کارهایی همچون اتوماسیون، مراقبت سلامت، بانکداری، انرژی، هوافضا، تولید صنعتی، خرده فروشی، امنیت و نظارت، شهرهای هوشمند، محیط زیست و تدارکات می باشد. جمع آوری و تبادل داده منجر به شکل گیری بنیان IoT می شود. در دهه اخیر، ما از طریق اضافه کردن قابلیت اشتراک گذاری داده ها، موفق به افزودن ارزش اشیاء و تبدیل آنها به ابزارهای پاسخگو شده ایم. این امر موجب ارتقای سطح ارزش اشیاء ساده از وضعیت عادی به یک معماری نوین IoT شده و یک لایه جدید به دنیای دیجیتالی امروز اضافه نموده است IoT. صنعتی یک فرصت چند میلیارد دلاری برای شرکت ها می باشد. در اینجا ۴ جنبه کلیدی یک شبکه IoT را ارائه شده که به شما کمک می کند نیازهای تجاری خود را برآورده ساخته و خود را با این فناوری به روز کنید: ساختار اینترنت اشیاء لایه زیرین ساختار اینترنت اشیاء IoT از لایه دستگاه تشکیل شده است. انتخاب سخت افزار و لوازم جانبی مناسب، در کنار حسگرهای مورد نیاز برای برآورده کردن نیازهای تجاری شما، نکته ای کلیدی است. دستگاه ها ممکن است انواع مختلفی داشته باشند، اما برای اینکه یک دستگاه IoT باشد، باید دارای برنامه های ارتباطی باشد و بتواند بطور مستقیم یا غیر مستقیم به اینترنت متصل شود. برخی از دستگاه ها به سامانه عامل نیاز ندارند[۱].

۴- معماری اینترنت اشیاء

اینترنت اشیا (IoT) به بخشی جدایی ناپذیر از زندگی مدرن تبدیل شده است و دستگاه ها و داده ها را به یکدیگر متصل می کند تا کارایی، اتوماسیون و کنترل بیشتری را ارائه دهد. در قلب این انقلاب تکنولوژیکی، معماری IoT نهفته است، یک سیستم پیچیده از دستگاه‌ها و نرم‌افزارهای متصل به هم که امکان تبادل یکپارچه اطلاعات را فراهم می‌کند. به‌طورکلی در حال حاضر معماری استانداردی در سطح جهانی برای اینترنت اشیا طراحی و ساخته نشده است و به همین علت نیز توضیح در خصوص معماری اینترنت اشیا می‌تواند کمی سخت و مشکل‌ساز باشد. اگر بخواهیم به طورکلی در خصوص این موضوع صحبت کنیم می‌توان گفت که معماری IoT به طور کامل به نحوه عملکرد و پیاده‌سازی اجزا و بخش‌های مختلف آن بستگی دارد. بااین‌حال، یک فرایند اساسی در این زمینه وجود دارد که اینترنت اشیا دقیقاً بر پایه و اساس آن ساخته شده است.این معماری که امروزه با نام معماری چهار لایه اینترنت اشیا نیز نامیده می‌شود.

۴-۱- لایه حسگرها

سنسورهایی که در تجهیزات و دستگاه‌ها مورد استفاده قرار می‌گیرند اولین لایه از معماری اینترنت اشیا را تشکیل می‌دهند. این سنسورها و حسگرها قادر هستند از طریق پارامترهای فیزیکی و محیطی که برای آنها تعریف شده است داده‌ها را دریافت کرده و

[1] IOT= Internet of Things

آنها را پردازش کنند. از طرف دیگر آنها قادر هستند که این اطلاعات و داده‌های جمع‌آوری شده را از طریق شبکه به سایر تجهیزاتی که در دنیای اینترنت اشیا به کار می‌روند نیز منتشر کنند. این لایه از معماری IoT از اهمیت بسیار زیادی برخوردار است؛ چراکه اگر اطلاعات و داده‌های جمع‌آوری‌شده دقت بالایی نداشته باشند نمی‌توان اطلاعات مناسبی را از آن‌ها استخراج کرد و همین عامل نیز باعث عملکرد نادرست کل سیستم خواهد شد.

۴-۲- لایه شبکه

لایه شبکه در انتقال داده‌هایی که از حسگرها جمع آوری می‌شود نقش کلیدی و بسیار مهمی را ایفا می‌کند. در این لایه سیستمی با نام سیستم DAS[1] تعریف شده که فرآیند تجمیع و تبدیل داده‌ها را انجام می‌دهد. از طرف دیگر این سیستم می‌تواند عملیات تبدیل داده‌های آنالوگ حسگرها به داده‌های دیجیتال مورد نیاز در سایر تجهیزات را انجام دهد. بسیاری از عملکردهای اساسی در سیستم‌های اینترنت اشیا مانند محافظت در برابر بدافزارها، فیلترکردن اطلاعات و گاهی اوقات تصمیم‌گیری بر اساس داده‌های ورودی و خدمات مربوط به مدیریت داده‌ها در همین لایه انجام می‌شود. پس لایه شبکه را نیز می‌توان از جمله لایه‌های بسیار مهم در معماری IoTبه شمار آورد.

۴-۳- لایه پردازش داده

این لایه از معماری اینترنت اشیا در واقع وظیفه پردازش اکوسیستم اینترنت اشیا را برعهده دارد. در این بخش داده‌ها از قبل از طریق لایه شبکه به مرکز تجزیه‌وتحلیل داده ارسال شده‌اند و داده‌های دریافت شده با استفاده از برنامه‌های نرم‌افزاری که اغلب به‌صورت تجاری طراحی شده و مبتنی بر هوش مصنوعی و تکنیک‌های یادگیری ماشین هستند استفاده می‌شود. داده‌های دریافت‌شده در این بخش پردازش شده و بینشی کلی از طریق آن‌ها به دست می‌آید که این بینش می‌تواند برای تصمیم‌گیری‌های آینده تجهیزات اینترنت اشیا مفید و سودمند باشد. این لایه در واقع نقش مغز را در معماری IoT ایفا می‌کند و به همین علت نیز عملکرد درست آن از اهمیت زیادی برخوردار است که برای داشتن چنین عملکردی حتماً باید از نرم‌افزارهای استاندارد و قوی استفاده کرد.

۴-۴- لایه اپلیکیشن

آخرین لایه از معماری چهار لایه‌ای اینترنت اشیا مربوط به لایه اپلیکیشن است. این لایه که با نام‌های مرکز داده یا مرکز ابری نیز شناخته می‌شود در واقع مدیریت داده‌ها را انجام می‌دهد. داده‌ها زمانی که دریافت شده و توسط لایه‌های قبلی پردازش می‌شوند وارد این لایه شده و سیستم‌های تصمیم‌گیری روی داده‌ها عملیاتی را انجام می‌دهند. در واقع این لایه همان لایه‌ای است که با کاربران نهایی در ارتباط است. این لایه بر اساس نوع کاربرد اینترنت اشیا در صنایع مختلف از جمله کشاورزی، مراقبت‌های بهداشتی، هوا و فضا و ... عملکرد متفاوتی خواهد داشت. معماری اینترنت اشیا به‌طورکلی از چهار لایه مختلف تشکیل شده است که این چهار لایه شامل موارد زیر هستند:

- لایه حسگرها که وظیفه دریافت اطلاعات را برعهده دارد.
- لایه شبکه که وظیفه انتقال داده‌های دریافت شده را برعهده دارد.
- لایه پردازش اطلاعات و داده‌ها که می‌تواند از داده‌های دریافت شده نتیجه‌گیری‌هایی را به دست بیاورد.
- و در نهایت لایه اپلیکیشن که به طور مستقیم با کاربر در ارتباط است هستند[۲].

عملکرد درست هریک از این لایه‌ها برای عملکرد درست تجهیزات اینترنت اشیا لازم و ضروری خواهد بود.

[1] Direct-Attached Storage

۵- ساختار مبتنی بر ابر

ازآنجاکه فعالیت‌هایی نظیر ذخیره‌سازی و پردازش داده‌ها بیشتر در دستگاه انجام می‌شود نه در ابر، این امر پیامدهای قابل‌توجهی برای IOT دارد. بسیاری از سیستم‌های IOT برای جمع‌آوری داده‌ها از تعداد زیادی سنسور استفاده می‌کنند و تصمیمات هوشمندی را اتخاذ می‌کنند. استفاده از ابر برای جمع‌آوری داده‌ها و ترسیم بینش از آن داده‌ها حائز اهمیت است. به‌عنوان‌مثال یک شرکت کشاورزی هوشمند می‌تواند حسگر رطوبت خاک را از کانزاس و کلرادو پس از کاشت همان دانه‌ها مقایسه کند. بدون ابر مقایسه داده‌ها در مناطق وسیع‌تر بسیار دشوار است. همچنین استفاده از ابر امکان مقیاس‌پذیری بالا را فراهم می‌آورد. وقتی صدها، هزاران یا حتی میلیون‌ها سنسور دارید، قرار دادن مقادیر زیادی از قدرت محاسباتی روی هر سنسور بسیار گران و پرانرژی است. در عوض، داده‌ها را می‌توان از طریق همه این سنسورها به ابر منتقل کرد و در آنجا به طور کلی پردازش کرد. مغز سیستم IOT در ابر قرار دارد. سنسورها و دستگاه‌ها داده‌ها را جمع می‌کنند و اقدامات را انجام می‌دهند اما پردازش / فرماندهی و تجزیه‌وتحلیل به طور معمول در ابر اتفاق می‌افتد.

در طول دهه گذشته، در هنگام به روزرسانی استراتژی های مدیریت داده و همچنین پیاده سازی فناوری های ساخت هوشمند، رایانش ابری به اولین انتخاب تبدیل شده است. تمام داده های جمع آوری شده از حسگرهای اطراف کارخانه به ابر یک مرکز داده از راه دور که در آن اطلاعات ذخیره ، مدیریت و پردازش می شود ارسال می شود. این فناوری دارای مزایایی برای اپراتورها است. در واقع با استفاده از یک سرویس مبتنی بر ابر، تولید کنندگان می توانند به راحتی از هر مکان ، داده های خود را مدیریت کرده و به آن دسترسی پیدا کنند. این مزیت برای نظارت از راه دور بر سایت های متعدد و البته به خصوص برای روند فعلی کار در خانه به خاطر همه گیری ویروس کرونا بسیار ایده آل است .با استفاده از cloud تولیدکنندگان می توانند داده های کارخانه هوشمند خود را بدون نیاز به سرمایه گذاری در راه اندازی افزارهای پر هزینه تجزیه و تحلیل کنند. در حقیقت، سرویس های ابری اغلب براساس هر بار استفاده و اجرا هزینه دارند، این بدان معناست که تولیدکنندگان فقط باید هزینه های مورد نیاز خود را پرداخت کنند و سیستمی دارند که به راحتی با تجارتشان مقیاس پذیر است. اما ذخیره داده ها در ابر خطراتی نیز دارد. برای مثال قطع شبکه باعث می شود تولیدکنندگان در صورت نیاز هم به داده های خود دسترسی پیدا نکنند. این یک چالش در برنامه هایی است که قابلیت ردیابی در آنها مهم است .همچنین نگرانی دیگر امنیت است، زیرا هر جابجایی داده باعث افزایش احتمال خطر حملات سایبری می شود .با ورود اینترنت اشیا به زندگی روزمره، ساکنان خانه های هوشمند می توانند دستگاه های خنک کننده را از راه دور از طریق تلفن همراه خود کنترل کنند که قبل از آن، این کار از طریق پیامک امکان پذیر بود اما در حال حاضر، اینترنت این کار را آسان کرده و اینترنت اشیا هم به عنوان یک ابزار به غیر از ارائه راهکارهای هوشمندانه برای خانه ها و جوامع مسکونی در محیط های تجاری صنایع مختلف نیز مورد استفاده قرار گرفته است. استفاده از ابر برای جمع آوری داده ها و ترسیم طرحی برای به کارگیری آن داده ها از اهمیت زیادی برخوردار است. به عنوان مثال، یک شرکت کشاورزی هوشمند می تواند حسگرهای رطوبت خاک ایالتهای کانزاس و کلرادو را پس از کاشت بذرهای مشابه مقایسه کند. اما بدون وجود ابر، مقایسه داده ها در مناطق وسیعتر بسیار دشوارتر است. استفاده از رایانش ابری قابلیت مقیاس پذیری بالا را نیز فراهم می کند .پس وقتی تعداد بیشماری سنسور داشته باشیم قرار دادن مقدار زیادی انرژی محاسباتی روی هر سنسور بسیار گران و پر مصرف است. ولی اگر داده ها بتوانند از طریق همه این حسگرها به ابر منتقل شوند پردازش می تواند در آنجا صورت گیرد .اینترنت اشیا در حال تولید داده های فراوانی است که فشار زیادی را به زیرساخت های اینترنت وارد می کند. در نتیجه، شرکت ها در حال تلاش برای یافتن راه کارهایی برای کاهش فشار و حل مشکل داده ها هستند که رایانش ابری با ساختن دستگاه های متصل به هم، بخش عمده ای از آن خواهد بود. اما تفاوت های چشمگیری بین رایانش ابری و اینترنت اشیا وجود دارد که در سال های آینده با تولید هرچه بیشتر داده ها، ایجاد خواهد شد. با این وجود، با تولید مقدار زیادی داده توسط اینترنت اشیا، فشارهای زیادی بر زیرساخت های اینترنت وارد می شود. این باعث شده است که مشاغل و سازمان به دنبال گزینه ای باشند که این بار را کاهش دهند.در حال حاضر، رایانش ابری تا حدودی در فناوری اطلاعات و زیرساخت های آن نفوذ کرده است و بسیاری از شرکت های بزرگ فناوری مانند آمازون، علی بابا، گوگل و اوراکل در حال

ساخت ابزارهای یادگیری ماشین با کمک فناوری ابری هستند تا طیف گسترده ای از راه حل ها را به مشاغل سراسر جهان ارائه دهند[۳].

۶- پروتکل های اینترنت اشیاء

پروتکل‌های اینترنت اشیا (IOT Protocols)بخش مهمی از تکنولوژی اینترنت اشیا هستند و بدون آنها سخت‌افزارها بدون استفاده می‌شوند چرا که پروتکل‌های IOT سخت‌افزارها را قادر می‌سازد تا داده‌ها به روشی ساختاریافته و معنادار مبادله شوند .وقتی صحبت از اینترنت اشیا می‌شود، ارتباط به ذهنمان می‌رسد. تعامل بین سنسورها، دستگاه‌ها، گیت‌ها، سرورها و برنامه‌های کاربردی کاربر، ویژگی اساسی است که اینترنت اشیا را شکل می‌دهد. اما آنچه که این چیزهای هوشمند را قادر می‌سازد تا با یکدیگر ارتباط برقرار کنند، پروتکل اینترنت اشیا است که می‌توان آن را زبانی دانست که ابزار اینترنت اشیا برای برقراری ارتباط از آن استفاده می‌کند.

۶-۱- پروتکل برنامه‌های محدود شده(Constrained Application Protocol)

درحالی که زیرساخت‌های اینترنت موجود برای تمام دستگاه‌های IOT به طور رایگان موجود و قابل استفاده است، در اکثر موارد استفاده از اینترنت اشیا بسیار سنگین و پرمصرف است. پروتکل برنامه‌های محدودشده (COAP) برای ترجمه‌ی مدل HTTP طراحی شد تا بتوان از آن در محیط‌های محدودکننده دستگاه و شبکه استفاده کرد. پروتکل COAP اینترنت اشیا برای پاسخگویی به نیازهای سیستم‌های IOT مبتنی بر HTTP طراحی شده و برای برقراری ارتباط امن بین نقاط پایانی، بر پروتکل بسته داده کاربر (UDP) متکی است. با اجازه‌ی پخش و پخش چندگانه، UDP[1]می‌تواند داده‌ها را به چندین میزبان منتقل کند درحالی که سرعت ارتباط و استفاده از پهنای باند کم را حفظ می‌کند؛ این کار باعث می‌شود این پروتکل برای شبکه‌های بی‌سیمی که معمولا در محیط‌های ماشین به ماشین (M2M) با محدودیت منابع استفاده می‌شوند، مناسب باشد.

نکته مشترک دیگر COAP با HTTP معماری انتقال بازنمودی حالت (RESTful) است که از یک مدل تعاملی درخواست/پاسخ بین نقاط پایانی برنامه پشتیبانی می‌کند. بعلاوه، پروتکل COAP اینترنت اشیا از روش‌های اولیه دریافت، ارسال، قرار دادن و حذف HTTP استفاده می‌کند که به لطف آن می‌توان در هنگام ارتباط بین بخش‌ها از ابهام جلوگیری کرد. پروتکل CoAP دارای کیفیت خدمات است که برای کنترل پیام‌های ارسال‌شده استفاده می‌شود و آنها را به عنوان «قابل تایید» یا «غیرقابل تایید» مشخص می‌کند و نشان می‌دهد آیا دریافت‌کننده باید تایید را بازگرداند یا خیر.

۶-۲- پروتکل انتقال تله‌متری صف‌بندی پیام‌ها(Message Queuing Telemetry Transport)

احتمالا گسترده‌ترین استاندارد استفاده شده در اینترنت اشیاء صنعتی تا به امروز، پروتکل انتقال تله‌متری صف‌بندی پیام‌ها (MQTT) است؛ یک پروتکل پیام‌رسان سبک وزن از نوع انتشار و اشتراک .(pub/sub) این پروتکل برای دستگاه‌های مبتنی بر باتری طراحی شده و معماری آن ساده و سبک‌وزن است که باعث مصرف کم‌تر انرژی در دستگاه‌ها می‌شود. پروتکل MQTT روی پروتکل TCP/IPکار شده و به ویژه برای شبکه‌های ارتباطی غیرقابل اعتماد طراحی شده است تا به مشکل تعداد فزاینده دستگاه‌های کم‌مصرف ارزان قیمت کوچک که در سال‌های اخیر در شبکه ظاهر شده‌اند، پاسخ دهد.

۶-۳- پروتکل MQTT در اینترنت اشیا

پروتکل MQTT مبتنی بر مدل اشتراک، انتشار و کارگذار است. در این مدل، وظیفه ناشر جمع‌اوری داده و ارسال اطلاعات به مشترکین از طریق لایه میانجی یعنی کارگذار است. از سوی دیگر نقش کارگذار تضمین امنیت با بررسی متقابل تایید ناشران و مشترکان است. پروتکل MQTT در اینترنت اشیا سه روش برای دستیابی به این امر ارائه می‌دهد (کیفیت خدمات) که به لطف آن ناشر می‌تواند کیفیت پیام خود را تعریف کند:

[1] User Datagram Protocol

- QoS0حداکثر یکبار: کمترین حالت اعتماد اما همچنین سریع‌ترین حالت است. انتشار ارسال شده است اما تاییدیه دریافت نشده است.
- QoS1حداقل یکبار: تضمین می‌کند که پیام حداقل یکبار تحویل داده شده است اما ممکن است موارد تکراری دریافت شود.
- QoS2دقیقا یکبار: قابل اعتمادترین حالت که در عین حال بیشترین پهنای باند را مصرف می‌کند. تکرارها کنترل می‌شوند تا اطمینان حاصل شود پیام تنها یکبار ارسال شده است.

۶-۳-۱- ویژگی‌ها، کاربردها و محدودیت‌های پروتکلMQTT

پروتکلMQTT در اینترنت اشیا کاربرد گسترده‌ای در دستگاه‌های اینترنت اشیا مانند کنتورهای الکتریکی، وسایل نقلیه، دتکتورها و تجهیزات صنعتی یا بهداشتی دارد و به نیازهای زیر به خوبی پاسخ می‌دهد:

- حداقل استفاده از پهنای باند
- عملیات از طریق شبکه‌های وایرلس یا بی‌سیم
- مصرف انرژی پایین
- قابلیت اطمینان خوب در صورت لزوم
- منابع پردازش و حافظه کم

پروتکل MQTT علیرغم ویژگی‌های آن، به خاطر انتقال پیام‌ها از طریق TCP و مدیریت نام‌های طولانی می‌تواند برای برخی دستگاه‌های محدودکننده، مشکل‌ساز باشد.البته این مشکل از طریق واریانت MQTT-SN که از UDP استفاده می‌کند و از نمایه‌سازی نام موضوع پشتیبانی می‌کند، قابل حل شدن است. با این حال، MQTT علیرغم پذیرش گسترده‌ی آن، از یک مدل ساختار مدیریت دستگاه و نمایش داده‌ی خوب که اجرای مدیریت داده و قابلیت‌های مدیریت دستگاه آن را کاملا مختص پلتفرم یا فروشنده می‌سازد، پشتیبانی نمی‌کند.

۶-۴- پروتکل وای فای(Wi-Fi)

ایجاد یک شبکه وای فای مستلزم دستگاه‌هایی است که بتوانند سیگنال‌های وایرلس ارسال کنند؛ دستگاه‌هایی مانند تلفن، کامپیوتر و روتر. در خانه از روتر برای انتقال اتصال اینترنت از شبکه عمومی به یک شبکه خانگی یا اداری خصوصی استفاده می‌شود. پروتکل وای فای (WiFi) یک اتصال اینترنت فراهم می‌کند تا دستگاه‌های نزدیک به آن که در محدوده خاصی قرار دارند، متصل شوند. راه دیگر برای استفاده از WiFi ایجاد یک نقطه اتصال یا Hotspot وای فای است؛ یعنی تلفن‌ها یا کامپیوترها می‌توانند با پخش یک سیگنال، اتصال اینترنت بی‌سیم یا سیمی را با دستگاه‌های دیگر به اشتراک بگذارند.

وای فای از امواج رادیویی استفاده می‌کند که اطلاعات را در فرکانس‌های مشخصی مانند ۲/۴ گیگاهرتز یا ۵ گیگاهرتز پخش می‌کند. هر دوی این محدوده فرکانس‌ها دارای تعدادی کانال هستند که دستگاه‌های بی‌سیم مختلف می‌توانند با آن کار کنند و به توزیع بار کمک می‌کنند تا اتصال‌های جداگانه قطع نشوند. این مساله تا حد زیادی از ازدیاد شبکه‌های بی‌سیم جلوگیری می‌کند. بُرد معمولی برای اتصال وای فای استاندارد حدودا ۱۰۰ متر است. با این حال، معمول‌ترین برد محدود به ۱۰ تا ۳۵ متر است. پوشش موثر شبکه تا حد زیادی تحت تاثیر قدرت آنتن‌دهی یا فرکانس انتقال است .محدوده و سرعت اتصال اینترنت وای فای بستگی به محیط و پوشش داخلی یا خارجی آن دارد. بنابراین، سرعت دستگاه‌های مختلفی که از اتصال اینترنت وای فای استفاده می‌کنند با نزدیک شدن به منبع اصلی افزایش می‌یابد و در مقابل با دور شدن از منبع نیز این سرعت کاهش می‌یابد.

۶-۵- پروتکل زیگبی(ZigBee)

شبکه‌های مبتنی بر ZigBee با مصرف انرژی کم، توان عملیاتی کم (حداکثر ۲۵۰ کیلوبیت در ثانیه) و محدوده اتصال ۱۰۰ متر بین گره‌ها شناخته می‌شوند.کاربردهای معمول استفاده از این پروتکل اینترنت اشیا شامل شبکه‌های حسگر، شبکه‌های شخصی

(WPAN)، اتوماسیون خانگی، سیستم‌های هشدار و سیستم‌های نظارتی می‌شود. مشخصات اولیه زیگبی به عنوان یک استاندارد IEEE در سال ۲۰۰۳ شناخته شد و اولین ماژول‌های OEM منطبق بر ZigBee در ابتدای سال ۲۰۰۶ به فروش انبوه رسید.

پروتکل زیگبی (ZigBee) به عنوان استانداردی برای شبکه‌های رادیویی خودپیکربندی و کوتاه‌برد و برای استفاده در سیستم‌های تله‌متری و ارتباط بین انواع سنسورها، دستگاه‌های نظارتی و همینطور خواندن بی‌سیم نتایج اندازه‌گیری کنتورهای انرژی و گرما و غیره، طراحی و ساخته شد. استاندارد ZigBee یک پروتکل نسبتا ساده، مقاوم در برابر خطاهای ارتباطی و خوانش‌های غیرمجاز و پروتکل تبادل داده‌های بسته است که اغلب در دستگاه‌هایی با نیازهای کم مانند میکروکنترلرها، سنسورها و غیره قرار داده می‌شود. نصب و نگهداری پروتکل ZigBee اینترنت اشیا آسان است زیرا این استاندارد مبتنی بر توپولوژی شبکه خودمونتاژ و خودترمیم‌شونده است. این استاندارد همچنین به راحتی به هزاران گره تبدیل می‌شود و امروزه تامین‌کنندگان زیادی هستند که دستگاه‌هایی مبتنی بر این استاندارد ارائه می‌دهند.

۶-۶- پروتکل بلوتوث(Bluetooth)

بلوتوث تکنولوژی‌ای است که به دستگاه‌های الکترونیکی مختلف مانند تلفن، کیبورد، کامپیوتر، لپ‌تاپ، موشواره، پرینتر، هدست یا بلندگو و غیره امکان اتصال بی‌سیم می‌دهد. به زبان دیگر می‌توان گفت تکنولوژی بلوتوث یک استاندارد باز است که در مشخصه‌ی IEEE 802.15.1 تعریف می‌شود و ویژگی‌های فنی آن شامل سه کلاس توان انتقال ERP 1-3 با محدوده‌ی به ترتیب ۱۰۰، ۱۰ و ۱ متر در فضای باز می‌شود. رایج‌ترین کلاس آن نیز مورد دوم یعنی ۱۰ متر است که به فرد امکان می‌دهد به دستگاه‌هایی در اتاق‌های مختلف و حتی در طبقات مختلف، متصل شوند. پروتکل بلوتوث از امواج رادیویی در باند فرکانسی ۲.۴ گیگاهرتز ISM استفاده می‌کند و دستگاهی که امکان استفاده از این استاندارد را فراهم می‌کند آداپتور بلوتوث است.

در تکنولوژی بلوتوث داده‌ها به صورت بسته به یکی از ۷۹ کانال (در مورد استاندارد بلوتوث ۱) با پهنای باند ۱مگاهرتز ارسال می‌شوند که حداکثر سرعت ۷۲۱ کیلوبیت بر ثانیه را ارائه می‌دهد. آخرین نسخه‌های بلوتوث (بلوتوث ۴)، 40کانال با پهنای باند ۲ مگاهرتز وجود دارد که سرعت انتقال داده‌ها در آن حداکثر ۳ مگابیت بر ثانیه است. لازم به ذکر است که استانداردهای بلوتوث جدیدتر که انتقال داده‌های سریعتر و ایمنی بیشتر ارائه می‌دهند با نسخه‌های قدیمی‌تر نیز سازگار هستند.

۶-۷- پروتکل پیام‌رسانی و حضور گسترش‌پذیر(Extensible Messaging and Presence Protocol)

پروتکل پیام‌رسانی و حضور گسترش‌پذیر (XMPP) در سال ۱۹۹۹ توسط انجمن منبع باز Jabber برای پیام‌رسانی فوری طراحی شد. این پروتکل امکان تبادل فوری داده‌های ساختاریافته اما قابل توسعه بین دو یا چند مشتری شبکه را فراهم می‌کند. XMPP از زمان آغاز به طور گسترده‌ای به عنوان یک پروتکل ارتباطی مورد استفاده قرار گرفته است. با گذشت زمان و ظهور مشخصات سبک‌وزن XMPP، یعنیXMPP-IoT ، در زمینه اینترنت اشیا نیز مورد استفاده قرار گرفت. نقاط قوت XMPP-IoT به عنوان یک استاندارد پشتیبانی‌شده منبع باز شامل قابلیت‌های آدرس‌دهی و مقیاس‌پذیری می‌شود که این استاندارد را برای اینترنت اشیاء مبتنی بر مصرف‌کننده، مناسب می‌سازد.

۶-۸- پروتکل سرویس توزیع داده‌ها(Data-Distribution Service)

پروتکل سرویس توزیع داده‌ها (DDS) بر اساس روش انتشار و اشتراک توسعه داده شده است. پروتکل DDS برای ارتباطات فوری ماشین به ماشین که توسط گروه مدیریت شیء (OMG[1]) طراحی شد، تبادل داده‌های مقیاس‌پذیر، قابل اعتماد، با کارآیی بالا و قابل تعامل را بین دستگاه‌های متصل مستقل از سخت‌افزار و پلتفرم نرم‌افزاری را امکان‌پذیر می‌سازد. این پروتکل از معماری بدون واسطه و چندپخش برای ارائه QOS باکیفیت بالا و اطمینان از ارتباط دستگاه‌ها استفاده می‌کند. معماری پروتکل DDS مبتنی بر لایه

[1] Object Management Group

انتشار-اشتراک داده محوری (DCPS[1]) و لایه (اختیاری) بازسازی محلی داده (DLRL[2]) است. درحالی که لایه DCPS مسئول توزیع داده آگاهانه، قابل مقایسه و کارآمد برای مشترکین است، DLRL رابطی برای عملکردهای DCPS ارائه می‌دهد که امکان انتقال داده‌ها بین اشیاء متصل به اینترنت اشیا را فراهم می‌کند.

۶-۹- پروتکل پیشرفته صف‌بندی پیام(Advanced Message Queuing Protocol)

پروتکل پیشرفته صف‌بندی پیام (AMQP) یک پروتکل از نوع انتشار/اشتراک استاندارد باز است که در سال ۲۰۰۳ ایجاد شد و ریشه در بخش خدمات مالی دارد. اگرچه این پروتکل در زمینه‌ی تکنولوژی ارتباطات اطلاعات جایگاه ویژه‌ای به دست آورده است اما استفاده از آن هنوز در صنعت اینترنت اشیا محدود است. این پروتکل ویژگی‌هایی مانند جهت‌گیری پیام، صف‌بندی، مسیریابی (از جمله سرتاسری و انتشار/اشتراک)، قابلیت اطمینان و امنیت را ارائه می‌دهد. احتمالا بزرگترین مزیت AMQP مدل ارتباطی قوی آن است. این پروتکل می‌تواند تراکنش‌های کامل را تضمین کند؛ اگرچه این ویژگی کاربردی است اما همیشه چیزی نیست که کاربردهای IoT به آن احتیاج داشته باشند. از آنجایی که AMQP سنگین است برای دستگاه‌های حسگر با حافظه، توان یا پهنای باند شبکه محدود مناسب نیست اما برای موارد خاصی از IOT می‌تواند تنها پروتکل قابل اجرا برای کاربردهای سرتاسری باشد؛ از جمله نمونه‌هایی مانند ماشین‌های صنعتی سنگین.

۶-۱۰- پروتکل شبکه سلولی(Cellular)

شبکه سلولی یکی از گسترده‌ترین و شناخته‌شده‌ترین گزینه‌های موجود برای برنامه‌های اینترنت اشیا است و یکی از بهترین گزینه‌ها برای مواردی است که ارتباط در فواصل طولانی‌تر مورد نیاز است. اگرچه استانداردهای سلولی قدیمی ۲ G[3]و ۳ Gامروزه در حال حذف شدن هستند اما شرکت‌های مخابراتی به سرعت در حال گسترش استانداردهای جدیدتر و سریع‌تر مانند ۴ G/LTEو ۵ G هستند. شبکه سلولی پهنای باند بالا و ارتباط قابل اطمینان را ارائه می‌دهد و قادر است مقادیر بالایی از داده‌ها را ارسال کند که برای بسیاری از کاربردهای IOT مهم است. با این حال، این ویژگی‌ها با هزینه‌ای همراه هستند که شامل قیمت بالاتر و مصرف بالاتر انرژی نسبت به سایر گزینه‌ها می‌شود[۴-۵].

۷- اهمیت پروتکل های اینترنت اشیاء

مزیت و ارزش اینترنت اشیا به خاطر توانمندسازی اجزای مختلف برای ارتباط با یکدیگر است؛ این توانایی برقراری ارتباط همان چیزی است که داده‌ها را از دستگاه‌های مختلف خط اینترنت اشیا دریافت کرده و به سرورهای مرکزی می‌رساند. این ارتباط از طریق پروتکل‌های اینترنت اشیاء اتفاق می‌افتد که تضمین می‌کند داده‌ها از دستگاه‌های نقطه پایانی مانند سنسورها دریافت شده و توسط مراحل بعدی‌تر در این محیط متصل درک می‌شوند؛ فارغ از اینکه مراحل بعدی آن داده، یک دستگاه نقطه پایانی دیگر باشد یا یک دروازه و یا یک اپلیکیشن. به زبان ساده می‌توان گفت پروتکل های اینترنت اشیا به اندازه خود چیزها برای وجود اینترنت اشیاء حیاتی هستند. اگرچه پروتکل‌ها به عنوان یک گروه جمعی برای عملکرد IOT ضروری هستند اما همه پروتکل‌ها به طور یکسانی ایجاد نمی‌شوند. همه پروتکل‌ها در هر شرایطی به خوبی کار نمی‌کنند و یا حتی می‌توان گفت همه آنها در یک شرایط یکسان کار نمی‌کنند. برخی از پروتکل‌های اینترنت اشیا برای استفاده از IOT درون ساختمان‌ها مناسب هستند؛ برخی برای استقرار اینترنت اشیا در بین ساختمان‌ها به خوبی کار می‌کنند و در نهایت برخی دیگر برای موارد استفاده از اینترنت اشیاء ملی یا جهانی کاربرد دارند[۵].

[1] Data-Centric Publish-Subscribe
[2] data local reconstruction layer
[3] generation

۸- نتیجه گیری

معماری اینترنت اشیا یک سیستم پیچیده و چندوجهی است که امکان تبادل یکپارچه داده ها بین دستگاه ها و ابر را فراهم می کند. یک معماری خوب طراحی شده برای موفقیت استقرار اینترنت اشیا، امکان انتقال کارآمد داده ها، افزایش امنیت و امکان توسعه سریع برنامه ها بسیار مهم است. با وجود معماری مناسب، سازمان‌ها می‌توانند بینش‌های ارزشمندی را از داده‌های اینترنت اشیا به دست آورند و از آن‌ها برای بهینه‌سازی عملیات خود و ارتقای تجربیات مشتری استفاده کنند. اگر به دنبال ارائه دهنده اینترنت پرسرعت در ایران برای پشتیبانی از استقرار اینترنت اشیا خود هستید، صفرویک، ارائه دهنده پیشرو خدمات اینترنت سریع و مطمئن را در نظر بگیرید. هیچ پروتکل ارتباطی واحدی به تنهایی بهترین نیست و همه پروتکل‌ها برای هر کاربردی مناسب نیستند. درواقع تکنسین‌های سازمانی باید بر اساس شرایط ویژه استقرار برنامه‌ریزی‌شدهIOT ، تعیین کنند کدام پروتکل اینترنت اشیا برای سازمان آنها مناسب‌تر است. در این تصمیم‌گیری باید طیف وسیعی از فاکتورها از نیاز به برق دستگاه‌های متصل و محل قرارگیری دستگاه‌ها، تا اندازه جغرافیایی و مشخصه‌های محل استقرار آنها و در نهایت ملزومات ایمنی در نظر گرفته شود. به همین دلایل است که توصیف و تعریف انواع پروتکل اینترنت اشیا مهم است.

۹- مراجع

1. Afzal, B., Umair, M., Shah, G.A., Ahmed, E., 2019. Enabling IoT platforms for social IoT applications: vision, feature mapping, and challenges. Future Generation Computer Systems 92, 718–731.

2. Anthi, E., Williams, L., Słowi´nska, M., Theodorakopoulos, G., Burnap, P., 2019. A supervised intrusion detection system for smart home iot devices. IEEE Internet of Things Journal 6, 9042–9053. doi:10.1109/JIOT.2019.2926365.

3. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., et al., 2017. Understanding the mirai botnet, in: 26th {USENIX} security symposium ({USENIX} Security 17), pp. 1093–1110.

4. Bawany, N.Z., Shamsi, J.A., 2019. Seal: Sdn based secure and agile framework for protecting smart city applications from ddos attacks.Journal of Network and Computer Applications 145, 102381.

5. Brewer, R., 2016. Ransomware attacks: detection, prevention and cure. Network Security 2016, 5–9.