جزوه اینترنت اشیاء

ردیف	ریز محتوا
۱	مفاهیم پایه، تعریف، اهمیت، دامنه های کاربرد، سیر تکامل، اکوسیستم، استانداردهای مطرح ،مزایا و چالشهای اینترنت اشیاء معماری و مدلهای مرجع اینترنت اشیاء زیرساخت اینترنت اشیاء دستگاهها، اشیاء، چیزها، حسگرها، عملگرها و... شبکه های حسگر بیسیم انواع استانداردهای شبکه های کامپیوتری در زیرساخت اینترنت اشیاء تعاملات، سازگاری و پروتکلهای مورد نیاز در لایه ارتباطات اینترنت اشیاء پلتفرمهای اینترنت اشیاء سرویسها و معماری سرویس گرا در لایه کاربرد اینترنت اشیاء آشنایی با چالشهای تطبیق Application ها آشنایی با چالشهای امنیتی و حریم خصوصی اینترنت اشیاء
۲	آشنایی و نحوه کار عملی با سختافزارهای اینترنت اشیاء، شامل: آشنایی و نحوه کار با انواع حسگرها، عملگرها، میکروکنترلرها
۳	آشنایی و نحوه کار عملی با پلتفرمهای سختافزاری متداول برای اینترنت اشیاء و نحوه برنامهنویسی با آنها مانند: Arduino،Raspberry Pi و...
۴	آشنایی با ماژولهای مورد نیاز شبکهای مانند: Ethernet، Wi-Fi، Bluetooth و ... و نحوه ارتباط آنها با پلتفرمهای سختافزاری
۵	آشنایی با ساختار و اجزاء BMS
۶	آشنایی با سیستم عامل اینترنت اشیاء، مانند: Contiki آشنایی با شبیه ساز اینترنت اشیاء مانند: Cooja
۷	انجام یک پروژه عملی اینترنت اشیاء

مفاهیم پایه:

معرفی اینترنت اشیا (IoT)

مفهوم اینترنت اشیا به ارتباط مجموعه‌ای از اشیا، دستگاه‌ها، انسان‌ها، حیوانات و ماشین‌آلات اشاره دارد که در آن تمامی عناصر علاوه بر ارتباط با عناصر هم جنس خود، می‌توانند با دیگر عناصر نیز ارتباط داشته باشند. در واقع اینترنت اشیا یک شبکه متصل و متشکل از چندین موجودیت است که توانسته با افزودن قابلیت پردازش داده و هوش مصنوعی، دنیای فیزیکی و سایبری را با یکدیگر ادغام و یکپارچه نماید و جهانی هوشمند را ایجاد کند.

اکنون به لطف توسعه بی سابقه حسگرها و دستگاه‌ها، شبکه‌های ارتباطی، فناوری‌های پردازشی، پلتفرم‌های داده‌ای و هوش مصنوعی به یک واقعیت در تمامی حوزه‌ها و صنایع تبدیل شده است. در واقع هر موجودیت هوشمندی که در چارچوب اینترنت اشیا قرار می‌گیرد فارغ از نوع عملکرد خود، قابلیت جمع‌آوری و به اشتراک‌گذاری لحظه‌ای داده را با سایر موجودیت‌ها و ذینفعان دارد و موجب می‌شود که تمامی عناصر با کمترین نیاز به تعاملات با انسان، نسبت به تصمیم‌گیری اقدام نموده و به انجام عملیات لازم بپردازند.

به‌طور کلی به اشیاء و تجهیزات محیط پیرامون‌مان که به شبکه اینترنت متصل شده و توسط اپلیکیشن های موجود در تلفن‌های هوشمند و تبلت قابل کنترل و مدیریت هستند، اشاره دارد. اینترنت اشیاء به زبان ساده، ارتباط حسگرها و دستگاه‌ها با شبکه ای است که از طریق آن می‌توانند با یکدیگر و با کاربرانشان تعامل کنند. این مفهوم می‌تواند به سادگی ارتباط یک گوشی هوشمند با تلویزیون، یا به پیچیدگی نظارت بر زیرساخت‌های شهری و ترافیک باشد. از ماشین لباسشویی و یخچال گرفته تا پوشاک؛ این شبکه بسیاری از دستگاه‌های اطراف ما را در برمی‌گیرد

اتحادیه بین‌المللی مخابرات ، اینترنت اشیاء را «زیرساختی جهانی برای جامعه اطلاعاتی که بر اساس فناوری‌های ارتباطی و اطلاعاتی دارای قابلیت تعامل‌پذیری از قبل موجود و رو به رشد از طریق اتصال (فیزیکی و مجازی) اشیاء خدمات پیشرفته‌ای را ممکن می‌سازد» تعریف کرده‌است.

طبق رهنمودهای اتحادیه بین‌المللی مخابرات «چیز» در عبارت اینترنت اشیاء یا به یک شی از جهان فیزیکی (اشیاءی فیزیکی) یا جهان اطلاعات (اشیاءی مجازی) اشاره دارد که قابلیت شناسایی شدن و یکپارچه گشتن با شبکه‌های ارتباطی را دارا است.

اینترنت اشیا اجازه می‌دهد تا اشیا در سراسر زیرساخت‌های شبکه موجود، از راه دور کنترل شوند و همچنین فرصت برای ادغام مستقیم از جهان فیزیکی به سیستم‌های مبتنی بر کامپیوتر ایجاد کرده‌است و در بهبود بهره‌وری، دقت و سود اقتصادی علاوه بر کاهش دخالت انسان منجر شده‌است که اینترنت اشیا با سنسورها و محرک‌ها تکمیل شوند که شامل تکنولوژی‌هایی مانند شبکه‌های هوشمند، نیروگاه مجازی، خانه‌های هوشمند، حمل و نقل هوشمند و شهرهای هوشمند تبدیل شوند.

هر چیز منحصر به فردی از طریق سیستم‌های محاسباتی جاسازی شده قابل شناسایی است. و قادر به همکاری در زیرساخت اینترنت موجود است.

کارشناسان تخمین می‌زنند که اینترنت اشیاء در حدود سی میلیارد شیء تا سال ۲۰۲۲ تشکیل خواهد شد.

اما به‌طور معمول، انتظار می‌رود که اینترنت اشیاء اتصال پیشرفته از دستگاه‌ها، سیستم‌ها و خدمات که فراتر از ارتباطات ماشین به ماشین (M ۲M) می‌رود، ارائه کند و و انواع پروتکل‌ها، دامنه‌ها و برنامه‌های کاربردی را پوشش می‌دهد.

انتظار می‌رود که اتصال این دستگاه‌های تعبیه شده (از جمله اشیای هوشمند) به اتوماسیون در تقریباً تمامی زمینه‌ها کمک کند، در حالیکه همچنین برنامه‌های کاربردی پیشرفته مانند شبکه هوشمند را قادر می‌سازد و به مناطق مانند شهرهای هوشمند گسترش می‌دهد.

تعریف : «چیز»، در عبارت اینترنت اشیاء، می‌توانند رجوع شود به طیف گسترده‌ای از دستگاه‌ها مانند ایمپلنت نظارت بر قلب، فرستنده زیست تراشه در حیوانات مزرعه، حلزون‌های الکتریکی در آب‌های ساحلی، خودروها با سنسورها، دستگاه‌های تجزیه و تحلیل دی ان ای برای نظارت بر محیط زیست/ مواد غذایی/ پاتوژن یا دستگاه‌های عملیات میدانی که به آتش نشانان در عملیات جستجو و نجات کمک می‌کند. دانشمندان حقوقی «اشیاء» را به عنوان یک « ترکیبی بد از سخت‌افزار نرم‌افزار اطلاعات خدمات» قلمداد می‌کنند.

این دستگاه‌ها اطلاعات مفید با کمک فناوری‌های مختلف موجود جمع‌آوری می‌کنند سپس به صورت خودکار داده‌ها را بین دستگاه‌های دیگر به جریان می‌اندازد. نمونه بازار کنونی عبارتند از اتوماسیون خانگی (همچنین به عنوان دستگاه‌های خانه‌های

هوشمند شناخته می‌شود مانند کنترل و اتوماسیون روشنایی، گرمایشی (مانند ترموستات هوشمند)، تهویه، سیستم‌های تهویه مطبوع(....) و لوازم خانگی از قبیل ماشین لباسشویی/ خشک کن، جاروبرقی روباتیک، تصفیه هوا، اجاق گاز، یخچال/ فریزر یخ کننده که با استفاده از وای فای برای نظارت از راه دور به کار می‌رود.

همچنین گسترش اتوماسیون متصل به اینترنت در بخش‌های نرم‌افزار جدید، انتظار می‌رود که اینترنت اشیا مقادیر زیادی از داده‌ها از مکان‌های مختلف با ضرورت نتیجه بخش تجمع سریع داده‌ها و افزایش نیاز به شاخصه فروشگاه و فرایند داده‌ها (به‌طور مؤثر) جمع‌آوری کند. اینترنت اشیا یکی از سیستم عامل‌های هوشمند شهر امروز و سیستم‌های مدیریت انرژی است.
اصطلاح اینترنت اشیا توسط کوین اشتوین در شرکت پراکتر و گمبل، بعد در مرکز دانشگاه **M I T** در سال ۱۹۹۹ ابداع شد .

تعریف های زیادی از اینترنت چیزها توسط انجمن‌های مختلف تحقیقاتی بر اساس نوع نگرش آن‌ها به نقاط قوت این ایده بیان شده‌است. دلیل چند وجهی بودن این مفهوم به نام‌گذاری این ایده یعنی «اینترنت اشیا» برمی گردد.

این نام از دو کلمه تشکیل شده‌است، کلمه اول به دیدگاه شبکه گرایی این مفهوم تأکید دارد درحالی که کلمه دوم به حرکت به سمت اشیاء عمومی که در یک بسته مشترک قرار گرفته‌اند تأکید می‌کند. اینکه به اینترنت اشیا با دید اینترنت گرا یا موجودیت گرا نگاه کنیم باعث به وجود آمدن تغییر در ذینفعان، قراردادهای تجاری، تحقیق‌ها و استانداردهای موجود خواهد شد. در طراحی معماری آن Auto-ID Center مؤسسه فناوری ماساچوست MIT نیز مشارکت داشت.

تعاریف مختلف اینترنت اشیا

اینترنت اشیا را می‌توان از منظرهای مختلفی نیز تعریف نمود و هر یک از سازمان‌های تدوین استاندارد تعاریف متفاوتی را ارائه کرده‌اند.

ISO/IEC: اینترنت اشیا یک زیرساخت متصل متشکل از اشیا، افراد، سیستم‌ها، منابع اطلاعاتی و خدمات هوشمند است که به آن‌ها امکان می‌دهد اطلاعات حاصل از دنیای فیزیکی و مجازی را با یکدیگر ترکیب کرده و با استفاده از پردازش‌ها، واکنش‌های مناسب را ایجاد کند.

ITU-T Y.۲۰۶۰: اینترنت اشیا یک زیرساخت جهانی برای جامعه اطلاعاتی است که امکان ارائه خدمات پیشرفته را از طریق اتصال میان عناصر (فیزیکی و مجازی) موجود و فناوری‌های ارتباطی و اطلاعاتی پیشرفته فراهم می‌آورد.

IEEE: اینترنت اشیا یک چارچوب است که در آن هر یک از عناصر نقش خاصی را بر عهده دارند و به اینترنت متصل هستند. به طور ویژه، هدف اینترنت اشیا این است که با ایجاد پلی میان دنیای مجازی و فیزیکی، خدمات و کاربردهای جدیدی را ارائه دهد و این در حالی است که ارتباطات ماشین به ماشین (M۲M) فقط ارتباطات پایه‌ای را میان اشیا و ابر را ایجاد می‌کند.

کاربرد اینترنت اشیا چیست؟

دامنه های کاربرد بسیار گوناگونی وجود دارد که تحت تأثیر اینترنت اشیا قرار میگیرد. این دامنه های کاربرد بر اساس دسترسی به شبکه، پوشش و مقیاس تقسیم بندی میشوند.

مصارف شخصی و خانگی

اطلاعات جمع آوری شده از طریق حسگرها فقط از طریق شخص مالک شبکه مورد استفاده قرار میگیرد. معمولاً از Wi-Fi به عنوان ستون اصلی این شبکه جهت انتقال تصاویر و صوت استفاده میشود. از جمله کاربردهای این حوزه میتوان به کاربردهای سلامت فراگیر)اندازه گیری پارامترهای سلامتی و مدیریت این پارامترها توسط نرم افزارهای ذیربط(، سامانه های پایش منزل)جهت پایش سلامت اشخاص مسن(، کنترل وسائل منزل از راه دور و سایر موارد مشابه اشاره کرد. این مصارف باعث تعامل مصرف کنندگان با اینترنت اشیا خواهد شد.

مصارف سازمانی

اطلاعات جمع آوری شده از این شبکه توسط مالکین سازمان استفاده میشود و میتواند به صورت انتخابی در اختیار دیگران قرار گیرد. پایش محیط یکی از کاربردهای اولیه این حوزه است که جهت نگهداری رکورد تعداد افراد ساکن در سازمان و مدیریت خدمات سازمان از آن استفاده میشود. یکی از کاربردهای اینترنت اشیا که در حال حاضر بسیار مورد توجه است ‘‘محیط هوشمند’’ است که شامل زیر سامانه هایی است که در جدول اول به همراه ویژگی های هر کدام نمایش داده شده است.

کاربردهای موجود در محیط شهری که میتواند از تحقق قابلیت های یک شبکهٔ حسگر بیسیم در شهر بهره مند شود نیز در جدول دوم نمایش داده شده است. این کاربردها بر اساس حوزه اثر خود گروه بندی شده اند.

	خانه/اداره هوشمند	خرده فروشی هوشمند	شهر هوشمند	کشاورزی/جنگل کاری هوشمند	آبیاری هوشمند	حمل و نقل هوشمند
اندازه شبکه	کوچک	کوچک	متوسط	متوسط/بزرگ	بزرگ	بزرگ
کاربران	خیلی کم (اعضای خانواده)	کم (سطح جامعه)	زیاد (قانون گذاران، عامه مردم)	کم (مالکین زمین، قانون گذاران)	کم (دولت)	بسیار زیاد (عامه مردم)
انرژی	باطری قابل شارژ مجدد	باطری قابل شارژ مجدد	باطری قابل شارژ مجدد، ذخیره انرژی	ذخیره انرژی	ذخیره انرژی	باطری قابل شارژ مجدد، ذخیره انرژی
اتصالات اینترنت	WiFi, 3G, 4G LTE	WiFi, 3G, 4G LTE	WiFi, 3G, 4G LTE	WiFi، ارتباطات ماهواره ای	ارتباطات ماهواره ای، پیوندهای مایکرو ویو	WiFi، ماهواره
مدیریت دادها	سرور محلی	سرور محلی	سرور اشتراکی	سرور محلی، سرور اشتراکی	سرور اشتراکی	سرور اشتراکی
دستگاه های اینترنت اشیاء	RFID، شبکه های حسگر بی سیم	RFID، شبکه های حسگر بی سیم	RFID، شبکه های حسگر بی سیم	شبکه های حسگر بی سیم	حسگرهای واحد	RFID، شبکه های حسگر بی سیم، حسگرهای واحد
نیازمندی پنهای باند	کم	کم	بزرگ	متوسط	متوسط	متوسط/بزرگ
مثال های بستر تست	منزل آگاه	مرکز خرده فروشی SAP	Smart Santander, citySense	SisVia	GBROOS, SEMAT	تعدادی پیاده سازی آزمایشی محدود

حوزه‌های کاربرد محیط هوشمند

	شهروندها
سلامت	ارزیابی پزشکی، پایش بیماران، پایش کارکنان، مدل سازی انتقال بیماری و روش های پیشگیری از آن (پایش برخط وضعیت سلامت و استفاده از اطلاعات پیش گویانه جهت کمک به پزشکان در کنترل بیماری یا کمک در جهت اخذ تدابیر لازم در سناریو بیماری های همه گیر)
خدمات اضطراری، دفاعی	پایش کارکنان از راه دور (سلامت و موقعیت)، مدیریت و توزیع منابع، برنامه ریزی واکنش، حسگرهای نصب شده در زیرساخت ساختمان ها جهت راهنمائی اشخاص حاضر در سناریوهای اضطراری و سوانح
پایش جمعیت	پایش جریان جمعیت جهت مدیریت فوریت ها، استفاده بهینه از فضاهای عمومی و خرده فروشی، گردش کار در محیط های تجاری
	حمل و نقل
مدیریت ترافیک	حمل و نقل هوشمند از طریق بهینه سازی زمان حقیقی اطلاعات مسیر و ترافیک
پایش زیرساخت ها	حسگرهای نصب شده درون زیرساخت ها جهت پایش فرسودگی ساختارها و سایر مباحث نگهداری، پایش تصادفات جهت مدیریت حوادث و هماهنگی پاسخ دهی اضطراری
	خدمات
آب	مدیریت کیفیت آب، نشت آب، مصرف آب، پخش آب، هدر رفتن آب
مدیریت ساختمان	کنترل حرارت، کنترل رطوبت، پایش فعالیت ها جهت مدیریت مصرف انرژی، مدیریت دستگاه های گرمایشی، هوادهی، تهویه هوا (HVAC)
محیط	مدیریت آلودگی هوا، پایش نویز، آبراه ها، پایش صنایع

کاربردهای بالقوه اینترنت اشیا در شهر ملبورن

خدمات

اطلاعات به دست آمده در این حوزة کاربرد معمولاً برای بهینه سازی خدمات استفاده میشود. این اطلاعات توسط شرکتهای خدماتی برای مدیریت منابع در جهت بهینه سازی هزینه در مقابل سود مورد استفاده قرار میگیرد. این کاربرد نیازمند شبکه های بزرگ و دقیق جهت پایش خدمات حساس و مدیریت کارای منابع است. شبکه مورد استفاده میتواند بین شبکه های سلولی، Wi-Fiو ماهواره ای تغییر کند. از جمله مثال های این حوزه میتوان به اندازه گیری هوشمند مصرف)پایش مداوم میزان مصرف(، سامانه های نظارت)ردگیری اهداف، فعالیتهای مشکوک، یافتن وسایل جا مانده(، پایش شبکه های آب)کنترل کیفیت آب شرب(و مشابه آن اشاره کرد.

حمل و نقل و لجستیک

حمل و نقل و لجستیک هوشمند به علت ماهیت اشتراک داده و زیرساخت مورد نظر جهت پیاده سازی در یک حوزه کاربرد قرار دارند. در این حوزه امکاناتی از جمله پایش زمان های مسافرت، انتخاب مسیر بهینه بین مبدأ و مقصد و سایر موارد مشابه فراهم شده است. اینترنت اشیا علاوه بر توسعه الگوریتم های بهبود کنترل ترافیک شهری، در حال کار بر روی سامانه های کنترلی چند منظوره است که از طریق آن علاوه بر اطلاعات به دست آمده از سامانه کنترل ترافیک شهری، اطلاعات معتبر و مرتبط در خصوص شرایط ترافیکی نیز به کاربر نمایش داده شود. یکی دیگر از کاربردهای این حوزه، مدیریت لجستیک است که شامل پایش ارسال محموله در کنار برنامه ریزی جهت ارسال کارای آن میباشد.

حمل و نقل لجستیک

IoTتقریبا در همه صنایع و به منظور هوشمند سازی کاربرد دارد، اما کاربرد اینترنت اشیا را می‌توان به دو بخش دیگر نیز تقسیم بندی کرد:

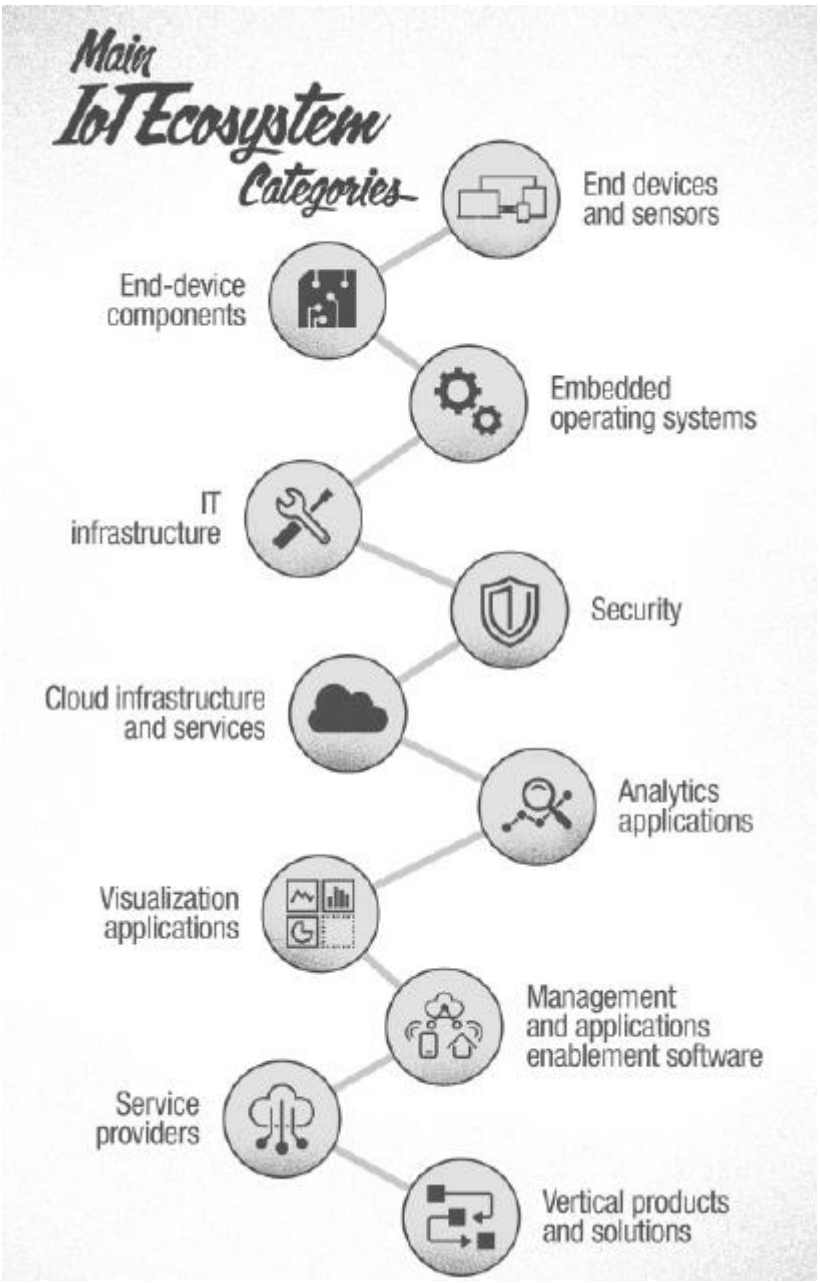
industry-specific offerings : یا پیشنهاد های مختص صنعت مانند حسگرها در یک کارخانه تولید کننده یا دستگاه های ارائه موقعیت مکانی بلادرنگ برای مراقبت های بهداشتی

IoT devices : که می‌توانند در تمام صنایع و یا سیستم های امنیتی مورد استفاده قرار گیرند.

در ضمن کاربرد دیگری که این حسگرها دارند این است که باعث می‌شوند شرکت ها درباره محصولات خود اطلاعات بیشتری کسب کنند و از آنها برای ساخت تجهیزات کارآمدتر استفاده کنند.

کاربرد دیگرIoT ، ارائه محیط تعاملی تر با قابلیت کنترل بیشتر است، ترموستات های هوشمند، سیستم نور خانه، سیستم های امنیتی و بسیاری ویژگی های دیگر باعث می‌شوند که بسیاری از فعالیت ها را بدون حضور فیزیکی کنترل کنیم.

ظهور اکوسیستم اینترنت اشیا



شما نمی توانید اینترنت اشیا را به تنهایی انجام دهید. در فصل اول کتاب بر توسعه یکپارچه یک اکوسیستم، به عنوان اولین مورد در موفقیت اینترنت اشیا تاکید شده است.

هیچ فروشنده ای به تنهایی نمی تواند یک راه حل کامل اینترنت اشیا برای هر مشتری فراهم آورد. اگر شما بخواهید به تنهایی این کار را انجام دهید، بسیار پرهزینه و پر خطر خواهد بود. اینترنت اشیا از طریق همکاری چند جز، ارزشی با بهره وری بیشتر را فراهم خواهد کرد که هر کدام از این مشارکت کننده ها ظرفیت و وظیفه مشخصی در تکمیل این ارزش دارند. Whitney Rockley مدیر سرمایه گذاری McRick Capital (شرکتی سرمایه گذار در حوزه اینترنت اشیا) بر افزایش مشارکت در اکوسیستم تاکید کرده است و به علت علاقمندی نسل جدید به حضور در استارت اپها، شرکتهای بلوغ یافته را به ایجاد همکاری با این شرکتهای نوپا تشویق می کند تا از ظرفیتهای آنان استفاده کنند تا هر دو طرف از این همکاری منفعت ببرند.

به واسطه اینترنت اشیا، صنایع به سرعت در شبکه ای از اکوسیستمهای تعاملی و مشارکتی بین کسب و کارها و مشتریان در حال توسعه هستند. بیشتر شرکتها برای توسعه راه حلهای بهینه با ماژول های قابل استفاده مجدد که هم باز هستند و هم متقابل، با مشتریان خود، همکاری می کنند. این یک تحول استراتژیک برای ارائه دهندگان سرویس و کاربران نهایی فناوری IoT است. نتیجه این یک اکوسیستم باز از مشارکت کنندگان مبتنی بر استاندارد برای راه حلهای اینترنت اشیا خواهد بود. ما این روند را اقتصاد همگانی می نامیم.

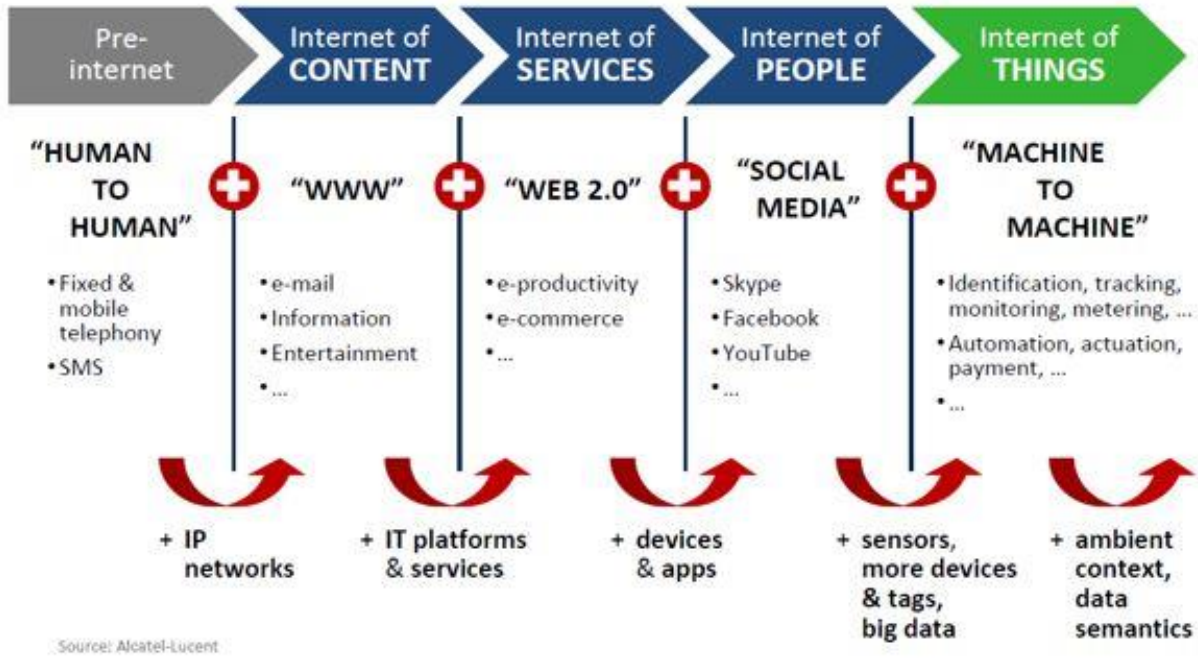
در دنیای امروز اکثر شرکتهای بزرگ مانند سیسکو دانسته اند که به تنهایی نمی توانند تمام کارها را انجام دهند و با مشارکت با بازیگران کلیدی می توانند سریعتر و زودتر به نتیجه دست پیدا کنند. به عنوان مثال FANUC با سیسکو و RockWell

Automation همکاری می کند و هر کدام وظیفه اصلی خود را انجام می دهند و اگر وظیفه اصلی مانده است که همچنان نادیده گرفته شده است، استارت اپها می توانند آن فضای خالی را پر کنند.

به گفته Sujjet Chad، مدیر فناوری شرکت RockWell، اینترنت اشیا یک بسته نیست و نمی توانید آن را از مغازه ها بخرید. یک شرکت به تنهایی نمی تواند آن را پیاده سازی کند، نه سیسکو، نه ما و نه هیچ شرکت دیگری.

سیر تکامل

تغییراتی که در تعامل و ارتباطات مابین موجودیت‌های (اشیاء) موجود در جهان، در طول زمان (قبل از ظهور اینترنت و بعد از ظهور اینترنت تا مطرح شدن ایده اینترنت اشیا) بوجود آمده، در شکل زیر به تصویر کشیده شده است.



شکل ۱- تغییرات اینترنت و ظهور اینترنت اشیا

همانطور که دیده می‌شوند تکامل در ارتباطات شامل مراحل زیر است:

قبل از اینترنت: ارتباطات انسان به انسان

اینترنت محتوا: وب نسل ۱ بر روی بستر شبکه‌های IP (اینترنت سنتی)

اینترنت سرویس: وب نسل ۲ و امکان تولید محتوا توسط کاربران

اینترنت افراد: شبکه‌ها و رسانه‌های اجتماعی

اینترنت اشیاء: اتصالات ماشین به ماشین

ارتباطات ماشین به ماشین (M۲M) اصطلاحی است که برای توصیف هر فناوری که دستگاه‌های شبکه را قادر به تبادل اطلاعات و انجام برخی عملیات بدون دخالت انسان می‌کند، به کار گرفته می‌شود. در واقع M۲M به عنوان بخشی از IoT در نظر گرفته می‌شود. پیش‌بینی‌ها نشان می‌دهد که تعداد اتصالات M۲M در سال‌های آینده رشد قابل توجهی خواهد داشت.

مفاهیم مرتبط به اینترنت اشیا سال‌ها قبل توسط مارک ویسر در شرکت زیراکس مطرح شده بود و در قالب حوزه پردازش (رایانش) فراگیر در حال رشد بود. هدف حوزه پردازش فراگیر شکل گیری جهانی است که در آن اشیاء اطراف ما (که به طور روزمره با آنها سروکار داریم) دارای قدرت پردازش بوده و به صورت بی سیم یا کابلی با شبکه جهانی در ارتباط باشند. دور نمای دیدگاه اولیه مارک ویسر دستیابی به سیستم های شبکه ای در حوزه فناوری اطلاعات و ارتباطات (ICT) است که نهفته در محیط پیرامون، پنهان از دید کاربر و خودکار می باشند. چنین سیستم هایی کاربر و فعالیت هایش را دنبال کرده و به نیازمندی های آن پاسخ می دهد. لذا به عبارتی کاربر را قادر می سازد با محیط فیزیکی اطرافش سازگار شود و سرویس هوشمندتری را دریافت کند (برای مثال، کاربردهای مکان محور).

از این مدل، به عنوان موج سوم پردازش اطلاعات یاد می‌شود. در موج اول (دوره کامپیوترهای بزرگ در دهه ۱۹۶۰) افراد زیادی مجبور بودند از یک کامپیوتر به طور مشترک استفاده کنند و در موج دوم (دهه ۱۹۸۰) هر فرد به یک کامپیوتر شخصی دسترسی داشت. اما در موج سوم (پیدایش ایده سیستم های فراگیر) هر فرد بطور خودکار و بدون اینکه تنظیمات خاصی انجام دهد، از کامپیوترهایی که در محیط اطرافش جاسازی شده اند (و از دید او پنهان هستند)، سرویس شخصی سازی شده می گیرد.

دیدگاه اولیه مارک ویسر، که در بالا به آن اشاره شد، تحولی را در دنیای ارتباطات دنبال می کند که طی سالیان اخیر بر روی جنبه های مختلف آن تحقیقات بسیاری توسط پژوهشگران در حوزه های مختلف انجام شده است. بطور کلی مطالعات انجام شده و جهت‌گیری های علمی در حوزه پردازش فراگیر را می‌توان در قالب سه نسل متفاوت بررسی کرد که در ادامه به آنها پرداخته می شود:

نسل اول پردازش فراگیر، که نسل "اتصال پذیری" نامیده می‌شود، سال های ۱۹۹۱ تا ۲۰۰۵ را شامل می شود. در این نسل، از پیشرفت های جدید در حوزه فناوری (همچون کوچک سازی تجهیزات الکترونیکی و مخابراتی، ارزان تر و قدرتمندتر شدن تجهیزات پردازشی، ارتباطی و ذخیره سازی، استانداردهای جدید ارتباطات بی سیم) برای دستیابی به ایده اتصال "هر چیزی به هر چیزی" بهره گرفته شده است. از مشخصات این نسل می توان به ساخت وسایل اطلاعاتی و پردازشی خاص منظوره، سیستم های سنسور-

عملگر برای تعاملات (ضمنی) مابین انسان و ماشین و معرفی قابلیت هایی چون خود پیکربندی، خودبهبودی، خودبهینه سازی و خودحفاظتی اشاره کرد.

نسل دوم سیستم های پردازش فراگیر، که نسل آگاهی نامیده می شود، بین سال های ۲۰۰۰ تا ۲۰۰۷ شکل گرفته است. این نسل بر پایه سیستم های تشخیص مبتنی بر سنسور و فناوری های جدید پردازش و ارایه دانش استوار می باشد. در این نسل، موضوعات تحقیقاتی ای چون سیستم های آگاه از زمینه و موقعیت، خودآگاه، آگاه از آینده یا آگاه از منبع، مورد تمرکز محققین بوده است. موجودیت هایی چون عوامل انسانی، شرایط محیطی و ابزارهای موجود در محیط که اطلاعاتی چون موقعیت مکانی، زمان، درجه حرارت، میزان روشنایی، میزان سر و صدا، نقش کاربر و اطلاعاتی نظیر نوع ارتباط شبکه ای از آنها بدست می آیند. لذا سیستم های آگاه از زمینه۱، سیستم هایی هستند که بطور فعال با موجودیت های محیط در تماس و تبادل اطلاعاتی هستند و فعالیت های خود را با استفاده از اطلاعات بدست آمده از محیط سازگار کرده و انجام می‌دهند. در نسل دوم، مفاهیمی چون خودمختاری و سازگاری بر مبنای دانش استخراج شده از داده های سطح پایین جمع آوری شده از سنسورها (در یک موقعیت مشخص یا دوره زمانی طولانی)، بنا گردید. نتیجه تحقیقات در این دوره، معرفی سیستم های خودمختار (و بعد از آن عناصر خودمختار) بودند که می‌توانستند اطلاعات و دانش زمینه را درک کنند، بطور خودکار خود را در تعامل با محیط توصیف، مدیریت و سازماندهی کنند و در نهایت رفتاری متناسب با دانش بدست آمده از خود نشان دهند.

با ظهور کاربردهای مختلف شبکه های اجتماعی در سال های اخیر، نحوه استفاده از اینترنت دچار تغییر اساسی شده است. امروزه میلیون ها کاربر بطور منظم به وب سایت هایی چون فیس بوک و توئیتر مراجعه کرده و از این طریق با دوستانشان در تماس بوده، به گروه های مورد علاقه خود ملحق می شوند، نظرات، افکار و پیشنهادات خود را منتشر می کنند و سایر اطلاعات مرتبط با خود را به روز نگاه می دارند. همچنان که افراد جدید به چنین شبکه های اجتماعی می پیوندند و از آن استفاده می کنند، اجتماعات مجازی شکل گرفته و ارتباطات اجتماعی آنلاین در فضای مجازی توسعه می یابند. علاوه بر این، افزایش رشد کاربران شبکه های تلفن همراه و ارایه گوشی های هوشمند با امکانات پیشرفته، منجر به شکل گیری پدیده ای مشابه (شبکه ای اجتماعی مابین افراد) در دنیای فیزیکی شده است. بطور مشخص، شبکه ای از وسایل (گوشی های تلفن همراه) بهم متصل شکل می گیرد که مجهز به انواع سنسورهای محیطی (برای ثبت و توصیف ارتباطات فیزیکی افراد، مکان آنها، فعالیت هایشان و مسیر حرکت آنها) می باشند. ترکیب زمینه موجود در شبکه های اجتماعی،که حاصل داده کاوی شبکه های اجتماعی است، با قابلیت های حسگری در تجهیزات ICT (همچون سنسورهای گوشی های هوشمند)، که حسگری فراگیر نامیده می شود، منجر به استخراج دانش کامل تری نسبت به موقعیت کاربران و سازگاری کاراتر کاربردهای فراگیر با نیازمندی های کاربران می گردد. اطلاعات حاصل از این ترکیب، زمینه اجتماعی فراگیر و حوزه ایجاد یا بکارگیری این نوع زمینه، پردازش اجتماعی فراگیر نامیده می شود. این حوزه یا بطورکلی تر ایده همگرایی فضای

مجازی و دنیای واقعی (Cyber-Physical Systems (CPS، در واقع نسل سوم پردازش فراگیر است که از سال ۲۰۰۸ آغاز شده است.

Advantages of Smart Homes	**مزایای خانه های هوشمند**
Increase in convenience	افزایش راحتی
Full control over all smart appliances with only one device	کنترل کامل بر روی تمام لوازم هوشمند تنها با یک دستگاه
Time savings	صرفه جویی در زمان
Higher quality of life	کیفیت زندگی بالاتر
Notifications in case of trouble	اطلاعیه در صورت بروز مشکل
Good tool to let people in from remote	ابزار خوبی برای اجازه دادن به افراد از راه دور
Energy savings	ذخیره انرژی
Cost savings in the long run	صرفه جویی در هزینه در بلندمدت
Smart homes can be customized to your needs	خانه های هوشمند را می توان بر اساس نیازهای شما سفارشی کرد
Safety improvements compared to conventional locks	بهبود ایمنی در مقایسه با قفل های معمولی
Insurance benefits	مزایای بیمه
Government subsidies and tax benefits for going green	یارانه های دولتی و مزایای مالیاتی برای سبز شدن
Support for the older generation	حمایت از نسل قدیمی
Smart homes may be suitable for disabled persons	خانه های هوشمند ممکن است برای افراد معلول مناسب باشند
Resale value might increase	ارزش فروش مجدد ممکن است افزایش یابد
May be fun for children to play around	ممکن است برای کودکان بازی در اطراف سرگرم کننده باشد

Disadvantages of Smart Home Technology	**معایب فناوری خانه هوشمند**
Significant installation costs	هزینه های قابل توجه نصب
Reliable internet connection is crucial	اتصال به اینترنت قابل اعتماد بسیار مهم است
Security issues	مسائل امنیتی
Technological problems in connected homes	مشکلات تکنولوژیکی در خانه های متصل
You may lock yourself out of your own house	ممکن است خود را در خانه خود حبس کنید
Helplessness if technology fails	درماندگی در صورت شکست فناوری
Some people may not like smart technologies	برخی از افراد ممکن است فناوری های هوشمند را دوست نداشته باشند
Maintenance and repair issues	مسائل مربوط به تعمیر و نگهداری
Some initial learning efforts necessary	برخی تلاش های اولیه برای یادگیری ضروری است
Compatibility problems between devices	مشکلات سازگاری بین دستگاه ها
Surges are possible	جهش ممکن است

Smart home technology not suitable for all houses	فناوری خانه هوشمند برای همه خانه ها مناسب نیست
Technology may become outdated soon	فناوری ممکن است به زودی منسوخ شود
Privacy concerns	نگرانی های حریم خصوصی

What are the advantages of IoT in business?	**مزایای اینترنت اشیا در تجارت چیست؟**
۱. Lower operating costs	۱. هزینه های عملیاتی کمتر
۲. Increased productivity	۲. افزایش بهره وری
۳. Better customer experiences	۳. تجارب بهتر مشتری
۴. More business insights	۴. بینش تجاری بیشتر
W**hat are the disadvantages of IoT in business?**	**معایب اینترنت اشیا در تجارت چیست؟**
۱. Security and privacy	۱. امنیت و حریم خصوصی
۲. Technical complexity	۲. پیچیدگی فنی
۳. Connectivity and power dependence	۳. اتصال و وابستگی به برق
۴. Integration	۴. یکپارچه سازی
۵. Time-consuming and expensive to implement	۵. زمان بر و پرهزینه برای اجرا

Advantages & Disadvantages of Smart Homes		**Top advantages and disadvantages of IoT in business**	
Disadvantages of Smart Home Technology	**Advantages of Smart Homes**	**What are the advantages of IoT in business?**	**What are the disadvantages of IoT in business?**
١-Significant installation costs	١-Increase in convenience	١. Lower operating costs	١. Security and privacy
٢-Reliable internet connection is crucial	٢-Full control over all smart appliances with only one device	٢. Increased productivity	٢. Technical complexity
٣-Security issues	٣-Time savings	٣. Better customer experiences	٣. Connectivity and power dependence
٤-Technological problems in connected homes	٤-Higher quality of life	٤. More business insights	٤. Integration
٥-You may lock yourself out of your own house	٥-Notifications in case of trouble		٥. Time-consuming and expensive to implement
٦-Helplessness if technology fails	٦-Good tool to let people in from remote		
٧-Some people may not like smart technologies	٧-Energy savings		
٨-Maintenance and repair issues	٨-Cost savings in the long run		
٩-Some initial learning efforts necessary	٩-Smart homes can be customized to your needs		
١٠-Compatibility problems between devices	١٠-Safety improvements compared to conventional locks		
١١-Surges are possible	١١-Insurance benefits		
١٢-Smart home technology not suitable for all houses	١٢-Government subsidies and tax benefits for going green		
١٣-Technology may become outdated soon	١٣-Support for the older generation		
١٥-Privacy concerns	١٤-Smart homes may be suitable for disabled persons		
	١٥-Resale value might increase		
	١٦-May be fun for children to play around		

مزایا و چالشهای اینترنت اشیاء

اینترنت اشیاء ، به عنوان انقلاب صنعتی بعدی معرفی می شود. یک تغییر بنیادی و یک الگوی کاملاً جدید برای کره زمین. به طور خاص ، IOTاز اتصالات موجود بین افراد و رایانه ها تا ‘‘اشیا’’ متصل به شبکه را شامل می‌شود. اما آیا تا به حال به مزایا و معایب اینترنت اشیا فکر کرده اید؟

IOTبا داده ها سروکار دارد. این داده ها می توانند اعدادی ساده از یک سنسور ثابت یا موبایل (مانند یک سنسور دما) تا یافته های پیچیده تری از دستگاه هایی باشند که چندین جریان داده را به طور همزمان اندازه گیری و گزارش می کنند.

هر فناوری جدید در مراحل اولیه خود با میلیون ها چالش روبروست. اما بگذارید فعلاً معایب را کنار بگذاریم و فقط در موارد مثبت در این فناوری متمرکز شویم.

مزایا اینترنت اشیا

قبل از فهمیدن تأثیر IoT در نحوه زندگی ما ، مهم است که از مزایا و معایب آن آگاه شویم:

ارتباطات

IoTارتباط بین دستگاه هایی را که به عنوان ارتباطات ماشین به ماشین (M۲M) نیز معروف است تقویت می کند. به همین دلیل ، دستگاه های فیزیکی هوشمند با شفافیت کامل ، ناکارآمدی کمتر و کیفیت بیشتر به ما سرویس دهی می‌کنند.

اتوماسیون و کنترل

به دلیل اتصال اشیاء به صورت دیجیتالی و مرکزی با زیرساخت های بی سیم ، اتوماسیون و کنترل زیادی در کارها وجود دارد. بدون دخالت انسان ، دستگاه ها قادر به برقراری ارتباط با یکدیگر هستند و منجر به خروجی سریعتر و به موقع می‌شوند.

اطلاعات

از دیگر مزایا اینترنت اشیا ، بالا رفتن میزان اطلاعات شماست. بدیهی است که داشتن اطلاعات بیشتر به تصمیم گیری بهتر کمک می‌کند. چه این اطلاعات راجع به نیازهای منزل برای خرید از فروشگاه مواد غذایی باشد، چه راجع به لوازم مورد نیاز در شرکتتان!

مانیتورینگ

چهارمین مزیت بارز IoT ، نظارت است. دانستن مقدار دقیق موادغذایی در یخچال یا میزان کیفیت هوا در خانه شما ، می‌تواند اطلاعات بیشتری را که قبلاً به راحتی قابل دسترس نبودند ، فراهم کند. به عنوان مثال ، دانستن کمبود شیر یا جوهر چاپگر می‌تواند در آینده نزدیک ، تحولی در نوع خرید کردن شما به وجود بیاورد! علاوه بر این ، نظارت بر انقضا موادغذایی باعث افزایش ایمنی خواهد شد.

زمان

همانطور که در مثالهای قبلی اشاره شد ، مقدار زمان صرفه جویی شده به دلیل وجود IoT ها بسیار بالاست و در زندگی مدرن امروز ، همه ما می توانیم از زمان بیشتری استفاده کنیم .پس انداز بزرگترین مزیت IoT صرفه جویی در هزینه است. با اتخاذ این فن آوری و نگه داشتن دستگاه ها تحت نظارت ، استفاده بهینه از انرژی و منابع حاصل می‌شود. در صورت وجود خرابی و خسارت احتمالی به سیستم ، می توانیم هشدار آن را دریافت کنیم. از این رو ، ما می‌توانیم با استفاده از این فناوری در هزینه خود صرفه جویی کنیم.

اتوماسیون کارهای روزانه و نظارت بهتر دستگاهها

IoTبه شما امکان می‌دهد تا انجام کارهای یکنواخت روزانه را بدون مداخلات انسانی به طور خودکار و کنترل کنید. اینترنت اشیا می تواند کیفیت خدمات را بالا برده و کمک کند تا در موارد اضطراری بهترین اقدامات لازم را انجام دهیم.

کیفیت بهتر زندگی

تمام کاربردها و مزایا اینترنت اشیا ، منجر به افزایش راحتی و مدیریت بهتر زمان و پول و انرژی می شوند و در نتیجه کیفیت زندگی ما به طرز چشمگیری بهبود می یابد.

معایب اینترنت اشیا

در اینجا ۷ مورد از معایب IoT آورده شده است:

سازگاری

در حال حاضر استاندارد بین المللی سازگاری برای اینترنت اشیا و نظارت بر آن وجود ندارد. من معتقدم که این نقطه ضعف به راحتی قابل رفع است. شرکت های تولید کننده این تجهیزات فقط باید با یک استاندارد مانند بلوتوث ، USBو غیره موافقت کنند. این چیز جدید یا ابتکاری شگفت آور نیست!

پیچیدگی

سیستم های پیچیده ، احتمال شکست بیشتری دارند. به عنوان مثال ، بیایید بگوییم که شما و همسرتان هرکدام یک پیام دریافت می‌کنید که می‌گوید شیر شما تمام شده است ، هر دو شیر خریداری می‌کنید. در نتیجه ، شما و همسرتان دو برابر مبلغ مورد نیاز خود را خریداری کرده اید. یا شاید یک اشکال نرم افزاری، به طور خودکار سفارش کارتریج جوهر جدید برای چاپگر خود را در هر ساعت و به مدت چند روز یا حداقل پس از هر قطعی برق ، هنگامی که فقط به یک کارتریج جایگزین نیاز دارید ، سفارش دهد.

حریم خصوصی / امنیت

از دیگر معایب اینترنت اشیا ، خطر از دست دادن حریم خصوصی است. به عنوان مثال ، داده ها چقدر خوب رمزگذاری و منتقل می شوند؟ آیا می خواهید همسایگان یا کارفرمایان شما بدانند که چه داروهایی را مصرف می کنید یا وضعیت مالی شما چگونه است؟ ما در نقشه اینترنت اشیا ،قبلا به طور مفصل درباره امنیت اینترنت اشیا نوشته ایم.

ایمنی

از آنجا که تمام لوازم خانگی ، ماشین آلات صنعتی ، خدمات بخش عمومی مانند تأمین آب و حمل و نقل و بسیاری از دستگاه های دیگر همه به اینترنت متصل هستند ، اطلاعات زیادی در مورد آن موجود است. این اطلاعات در معرض حمله هکرها قرار دارد. در صورت دستیابی به اطلاعات شخصی و محرمانه توسط متجاوزین غیرمجاز فجایع جبران ناپذیری به بار می‌آید.

سازگاری

به عنوان مثال در بخش کشاورزی، دستگاه های مختلف از تولیدکنندگان متفاوت خریداری می‌شود. اینجا مسئله سازگاری این دستگاه ها و نظارت بر آنها یکی از معایب اینترنت اشیا است. اگر همه تولید کنندگان با یک استاندارد مشترک موافقت کنند ، ممکن است این نقطه ضعف از بین برود ، اما حتی پس از آن ، مشکلات و مسائل فنی همچنان ادامه خواهد داشت. مشکلات سازگاری ممکن است منجر به خریدن تمامی تجهیزات از یک تولید کننده خاص شده و موجب ایجاد انحصار در بازار شود.

استخدام کمتر از نیروی انسانی

کارگران غیر ماهر ممکن است در اثر اتوماسیون و هوشمندسازی فعالیتهای روزمره شغل خود را از دست بدهند. با اتوماسیون فعالیت های روزانه ، به طور طبیعی ،افزایش نیروی انسانی ، کارگران و کارمندان با تحصیلات کمتر را به دنبال خواهد آورد. این می تواند به مشکلات بیکاری در جامعه منجر شود.

کنترل زندگی توسط IOT ها

زندگی ما به طور فزاینده ای توسط فناوری کنترل می شود و به آن وابسته خواهیم شد. نسل جوان در حال حاضر برای هر چیز کوچکی به فناوری اعتیاد دارد. ما باید تصمیم بگیریم که چقدر از زندگی روزمره خود را به دست مکانیزه کردن و کنترل فناوری بسپاریم.

دیدن نیمه پر لیوان بهتر است!

اگرچه IoT دارای معایب کمی است ، اما از مزایای آن در صرفه جویی در وقت و هزینه مصرف کننده نمی توان چشم پوشی کرد. بنابراین زمان زیادی نمی رسد که اینترنت اشیاء در تمامی خانواده ها و شرکت ها مشاهده شود. برای یافتن راه هایی برای مقابله با معایب آن باید تلاش کنیم.

اینها تنها چند مزیت اینترنت اشیاء است. بدیهی است که امکانات گسترده ای را برای ارتقاء کیفیت زندگی در همه جنبه ها باز می کند. اما ضروری است که ما دست روی نقاط مناسب بگذاریم تا این فناوری بهترین عملکرد را برای ما داشته باشد.

معماری اینترنت اشیا چگونه است ؟

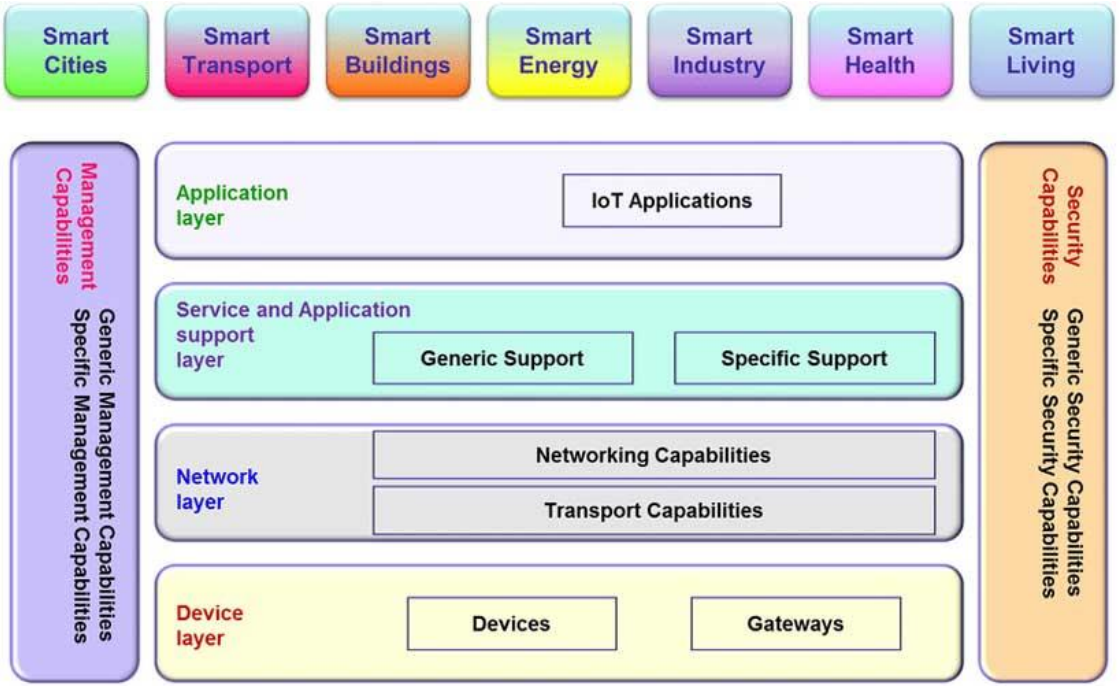
باید بدانید که اینترنت اشیا نیز مانند فناوری های دیگر ، نیاز به یک معماری واحد و استاندارد برای توسعه و پیشرفت دارد . در این بخش می خواهیم به بررسی کامل معماری در اینترنت اشیا بپردازیم و انواع مختلف معماری را در iot با یکدیگر بررسی کنیم .

اینترنت اشیا یا iot ساز و کار جدیدی است که قرار است زندگی بشر را هوشمند کند و شاهد عصر جدیدی از تحول تکنولوژی در زندگی انسان باشیم . در بخش های گذشته ، به کاربرد اینترنت اشیا در موارد گوناگون پرداختیم . و این موضوع را بررسی کردیم که چطور iot در پزشکی ، صنعت ، بانکداری ، آموزش و موارد دیگر تاثیر می گذارد . همچنین مزایا ، معایب و چالش ها را نیز بررسی کردیم .

یکی از چالش های اینترنت اشیا آن است که در حوزه های گوناگونی ظاهر شده است که هر کدام از آن ها دارای شرایط و چارچوبی خاص است . به همین دلیل شرکت ها و موسسه های گوناگون به فکر ایجاد یک معماری و پروتکلی واحد و یکسان برای iot افتادند. که در میان مدل های ارائه شده توسط هزاران شرکت مختلف ، دو نمونه ارائه شده توسط اتحادیه بین‌المللی مخابرات (ITU) و انجمن جهانی iot برتری ویژه ای دارند .

مدل معماری ITU

در شکل زیر میتوانید مدل ارائه شده توسط ITU را مشاهده کنید . همانطور که در این مدل می بینید ، چهار لایه اصلی افقی و دو لایه فرعی وجود دارد که به صورت عمودی وجود دارد . البته این دو لایه عمودی می توانند در هر لایه اصلی حضور داشته باشند . چراکه امنیت و مدیریت جزو اصلی ترین مسائل هر مرحله از کسب و کار است و تاثیر بسزایی در به موفقیت رسیدن آن امر دارد .



لایه اول مدل ITU

اول مربوط به وسایل مورد استفاده در اینترنت اشیا می شود . پروتکل های موجود در این لایه به بررسی مسائل مربوط به نوع و تعداد وسایل و ابزار هایی که در IOT هستند می پردازند .

لایه دوم مدل معماری

این لایه که network layer نام دارد مربوط به ارتباطات و انتقال دیتا ها است . در این لایه به نحوه تجهیزات شبکه ، پروتکل های اینترنت و به طور کلی ساز و کار انتقال دیتا پرداخته می شود .

لایه سوم معماری ITU

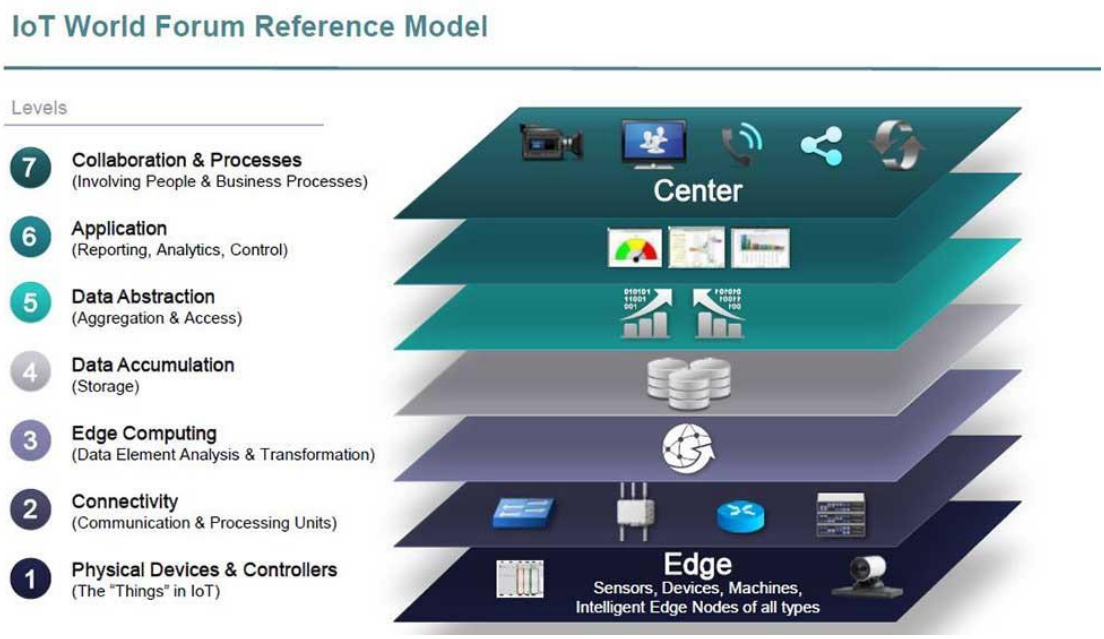
لایه سوم از مدل معماری اینترنت اشیا مربوط به پشتیبانی و Support تجهیزات و برنامه های کاربردی است . از وظایف این لایه می توان به سرویس و پشتیبانی محصولات و تجهیزات به صورت مداوم و بازگشتی اشاره کرد .

لایه چهارم ITU

لایه چهارم که لایه کاربر نیز نامیده می شود ، Application نام دارد . در این لایه مسائل مربوط به محصول نهایی بررسی می شوند . این لایه ، پل ارتباطی میان کاربر نهایی با لایه های زیرین است .

مدل معماری IOTWF

علاوه بر مدلی که توسط اتحادیه بین‌المللی مخابرات ارائه شده است ، مدل قابل قبول دیگری نیز به نامIOTWF وجود دارد که سازمان جهانی آن را طراحی کرده است . این مدل همانند مدل OSI دارای ۷ لایه می باشد که در شکل زیر میتوانید آن را مشاهده کنید. در انتها مقاله نسخه اصلیIOTWF هم میتوانید دانلود کنید.



این مدل در سال ۲۰۱۴ به همت تعداد زیادی از متخصصان و برنامه نویسان شرکت های بزرگی مانند سیسکو ، آی بی ام ، اپل و ماکروسافت طراحی و ارائه شد . از مزایای این مدل معماری می توان به سهولت ، یکپارچه سازی و کامل بودن آن اشاره کرد . ۷ لایه ای این مدل تقریبا همه مسائل مورد نیاز را پوشش داده اند که جزئیات هرکدام به شرح زیر است :

لایه اول IoTWF

لایه اول این مدل به بررسی اشیا و سنسور ها می پردازد . این لایه عملکرد مشابهی با لایه اول مدل قبلی دارد و پروتکل های مربوط به شی و وسایل در این لایه قرار می گیرد . و مسائلی مانند تنوع اشیا و قیمت آن ها در لایه اول معماری اشیا بررسی می شوند .

لایه دوم IoTWF

این لایه مربوط به مسائل ارتباطات و سوئیچینگ است . که مسائلی مانند نحوه استفاده از شبکه ها ، نوع تجهیزات شبکه و انواع مدل های ارتباط را تحت پوشش قرار می دهد .

لایه سوم IoTWF

لایه سوم مربوط به امور راینش و محاسباتی است . مطالعه بر بستر های ابری را میتوان از جمله اقدامات صورت گرفته در این لایه ذکر کرد . همچنین کاهش حجم بسته ها و فیلترینگ آن ها از جمله اقدامات دیگری است که در سطح لایه سوم صورت می گیرد .

لایه چهارم معماری IoTWF

لایه چهارم ، لایه انباشت نام دارد . در این قسمت از مدل IoTWF ، اقدامات و مطالعاتی درباره انباشت و ذخیره داده ها و اطلاعات انجام می شود . نحوه ذخیره سازی داده ها در انباره ها ، سرچ و واکاوی اطلاعات همگی در این لایه صورت می پذیرد .

لایه پنجم IoTWF

لایه پنجم که Data Abstract نام دارد . در این لایه داده هایی که در لایه های قبلی شکل گرفته اند ، منتقل شده اند و انبار گشته اند ، به شکل انتزاعی تر و نزدیک به واقعیت تبدیل می شوند . هنگامی که داده ها وارد لایه پنجم می شوند ، یکپارچه سازی و فرمت بندی می شوند . و به لایه ششم فرستاده می شوند .

لایه ششم IoTWF

در این لایه ، اطلاعات و داده ها تحلیل و آنالیز خواهند شد و کاربردی بودن یا نبودن آن به صورت هوشمند و یا دستی بررسی می شود . در این لایه دیتاها به هم پیوست می شوند و نتایج و گزارشات بدست می آید .

لایه هفتم IoTWF

این لایه ، که لایه کاربر نیز در معماری اینترنت اشیا نام دارد ، وظیفه انتقال و نمایش اطلاعات را به کاربر نهایی بر عهده دارد . اطلاعاتی را که در شش لایه قبلی به این لایه رسیدند ، پس از بررسی و کنترل به دست کاربر نهایی خواهد رسید .

سخن نهایی

همانطور که مشاهده کردید ، دو مدل از مهمترین معماری های کسب و کار را به شما توضیح دادیم البته معماری اینترنت اشیا به همین دو طرح خلاصه نخواهند شد و شرکت های دیگری نیز نظیر آمازون مدل هایی را ارائه کرده اند . اما هرگز به جامعیت و کاربردی بودن این دو مدل از معماری iot نخواهند رسید .

مدل مرجع اینترنت اشیاء :

یکی از چالش های مهم بکارگیری اینترنت اشیاء ، فقدان وجود یک مدل مرجع است که خوشبختانه در اکتبر سال ۲۰۱۴ در کنفرانس انجمن جهانی اینترنت اشیاء ، سیسکو با همکاری شرکت هایی نظیر IBM و Intel مدل مرجع اینترنت اشیاء را همانگونه که در شکل ۲ نشان داده شده است ، معرفی کرد .

در مدل فوق ، ایده جمع آوری ، مدیریت و تحلیل داده به بخش های کوچک تر متعددی تقسیم شده است . در این مدل مرجع ، فناوری های مختلف ، اجزاء سخت افزاری و نرم افزاری مربوطه ، نحوه ارتباط با یکدیگر ، محدوده های هر لایه به همراه اینترفیس های لایه های مختلف شناسایی تا امکان کار با محصولات چندین تولید کننده و تعامل بین لایه های مختلف به سادگی فراهم گردد .

با مطالعه این مدل ، اولین چیزی که به ذهن خطور پیدا می کند شباهت ایده و نگرش چندلایه ای آن با مدل معروف OSI است .

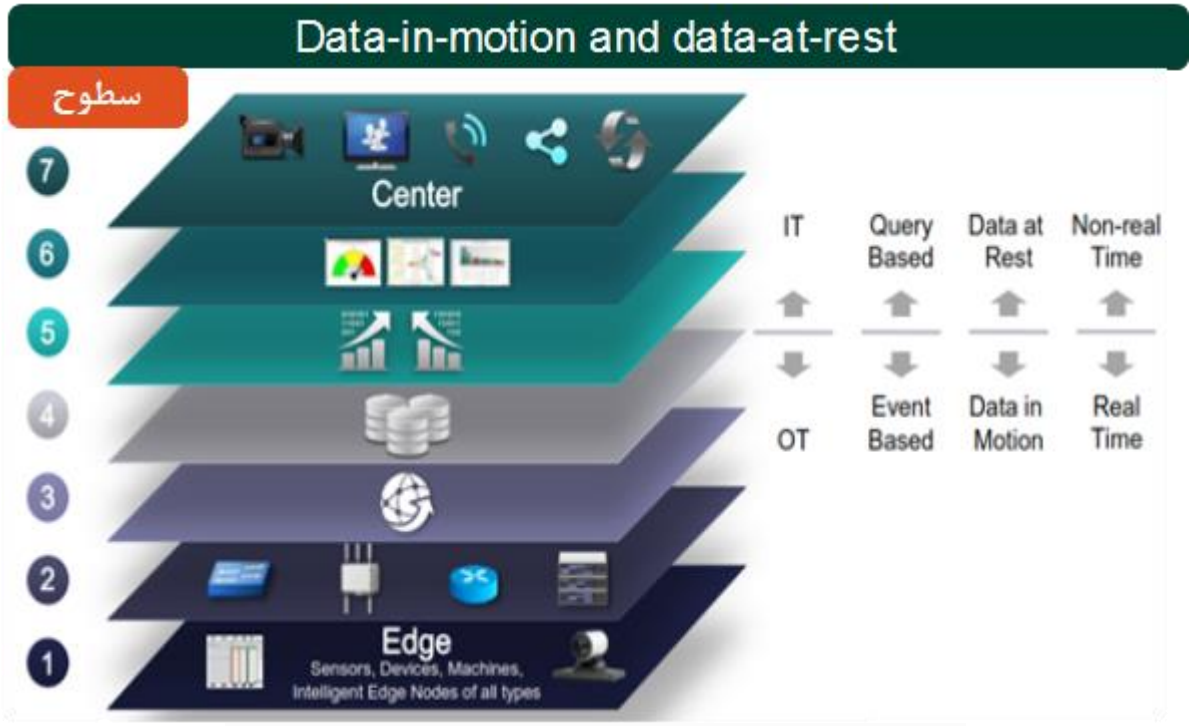
شکل ۲ : مدل مرجع اینترنت اشیاء (منبع سیسکو)

در پایین ترین لایه (لایه edge) ، ارتباط بین اشیاء تشریح می گردد . اشیاء به هر نوع دستگاه عملیاتی و یا عنصر اطلاق می گردد . یک سنسور دما و یا فشار در یک کارخانه ، یک دوربین امنیتی در یک فروشگاه خرده فروشی ، یک دستگاه نظارت بر فعالیت های پوشیدنی ، یک تلفن موبایل و یا هر نوع دستگاهی که از آن توسط یک فرآیند داخلی و یا یک مشتری و یا کانال شرکای تجاری به منظور هدایت کسب و کار و یا تعامل با دیگران استفاده می شود ، نمونه هایی در این زمینه می باشند .

لایه بعدی ، امکان اتصال بین تمامی این سنسورها و یا دستگاه های edge را با استفاده از یک gateway و یا یک لایه اتصال فراهم می نماید تا دستگاه های محلی را به یکدیگر متصل نماید .

در لایه بعد ، مفهوم edge-computing معرفی شده است. در این لایه ، کاربران داده بخصوصی را از دستگاه های edge و بر اساس مجموعه ای از قواعد به دست می آورند . این لایه دارای توانمندی لازم جهت هدایت تحلیل های محلی و تولید نتایج است که می تواند منجر به واکنش های محلی و بدون نیاز به ارسال داده به یک لایه بالاتر برای تحلیل آتی، گردد . این لایه را نمی توان

به منزله یک لایه تحلیل در نظر گرفت . در واقع لایه فوق ، یک لایه واکنش محلی است که امکان واکنش سریع و بلادرنگ را بر اساس داده در حال حرکت (data in motion) فراهم می نماید . در صورتی که فرآیندی به یک حد آستانه خاص که برای آن تعریف شده است نزدیک گردد، این لایه یک هشدار اولیه را و قبل از این که داده در لایه بالاتر پردازش گردد (لایه های تحلیلی) ، ارایه می نماید. در بازه زمانی فوق ، این لایه اقدام به ارسال یک واکنش مناسب به سمت لایه های پایین به منظور ضبط داده اضافی جهت بهبود نمونه ها و یا تشخیص روندها با درجه بالایی از صحت و دقت خواهد کرد .



Data-in-motion and data-at-restمنبع سیسکو : (شکل ۳)

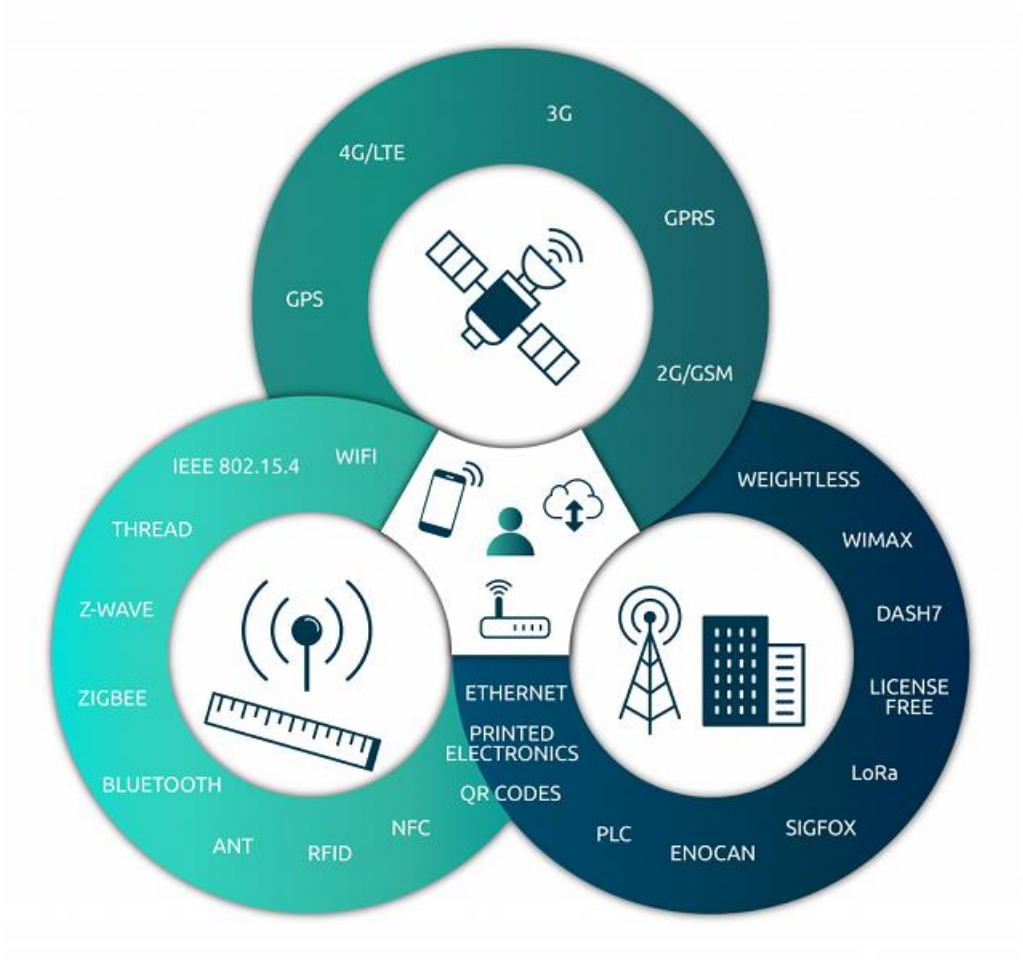
لایه های بالایی با مدیریت داده عملیاتی ، پردازش و توزیع آن برای تحلیل به نهادهای تجزیه و تحلیل جهت استخراج بینش سرو کار دارند. در اینترنت اشیاء ، جریان داده در دو جهت است . در یک الگوی کنترلی ، جریان اطلاعات کنترلی از بالا به پایین (سطح ۷) به سمت پایین (سطح یک) است و در یک الگوی مانیتورینگ ، جریان اطلاعات در اکثر سیستم ها بر عکس است و جهت جریان دو طرفه خواهد بود.

خلاصه

با توجه به رشد فراگیر و فزاینده اینترنت اشیاء ، نیاز به یک مدل مرجع بیش از همیشه احساس می شود . در پاسخ به این نیاز ، شرکت های پیشگام در حوزه فناوری بیکار ننشسته و تاکنون تلاش های متعددی را در این راه انجام داده اند . ارایه مدل مرجع اینترنت اشیاء در کنفرانس انجمن جهانی اینترنت اشیاء ، توسط سیسکو و شرکت های دیگری نظیر IBM و Intel یکی از تلاش های موفقیت آمیز اخیر است . در یک سیستمIoT ، داده توسط دستگاه های مختلفی تولید و با روش مختلفی پردازش و به مکان های مختلفی ارسال می گردد تا با توجه به نوع و ماهیت برنامه بر روی آنها کار شود . مدل مرجع اینترنت اشیاء پیشنهادی ، از چندین

سطح مختلف تشکیل شده است . هر سطح دارای واژگان اختصاصی مختص به خود که به نوعی استاندارد لازم جهت تعامل با سایر سطوح را در مدل مرجع مشخص می نماید . در این بخش ضمن اشاره به ضرورت وجود یک مدل مرجع برای اینترنت اشیاء با کلیات مدل مرجع ارایه شده توسط سیسکو آشنا شدیم . در بخش های بعدی با تمرکز بر روی هر لایه با ماموریت آن و همچنین شیوه تعامل با لایه های قبلی و بعدی آشنا خواهیم شد.

شبکه های تشکیل دهنده زیرساخت اینترنت اشیا



شبکه های تشکیل دهنده زیرساخت اینترنت اشیا

تکنولوژی و فناوری کاربردی اینترنت اشیا یا IOT که احتمالا تا الان نام آن را شنیده اید، برای ایجاد شبکه های مورد نیاز خود و اشتراک گذاری داده‌ها به زیرساخت هایی نیاز دارد. با توجه به طیف گسترده ای از موارد استفاده، برنامه‌ها و بایدها، طیف گسترده از تکنولوژی های ارتباطی وجود دارند که اپراتورها، دولوپرها، شرکت‌ها و مشتریان می‌توانند بر اساس خواسته خود انتخاب کنند. برای این که یک انتخاب درست و هوشمندانه صورت بگیرد، درک ویژگی‌های مختلف گزینه های ارتباطی ضروری به نظر می‌رسد. در ادامه با ما همراه باشید تا از مهم ترین جزئیات شبکه های تشکیل دهنده زیرساخت اینترنت اشیا باخبر شویم.

شبکه های بنیادین

تکنولوژی های ارتباطی اینترنت اشیا به دو بخش تقسیم بندی می‌شود که شامل شبکه های سلولی و شبکه های Low Power WAN است. جالب است که بدانید، فناوری اینترنت اشیا هنگامی که توسط شبکه های سلولی اینترنت اشیا مورد استفاده قرار بگیرد، این شبکه ی ارتباطی زیر ساخت مورد نیاز خود را از طریق منابع معتبر و سازگاری تامین می‌کند. شبکه های سلولی به طور معمول از بیگ دیتا، عمر باتری کم و سخت افزارهای ارزان قیمت می‌توانند پشتیبانی کنند. به همین دلیل است که راهکارهای مبتنی بر اینترنت اشیا که توسط اپراتورهای بزرگ ارائه شده است از این شبکه های سلولی برای زیر ساخت استفاده می‌کند.

در آن سوی ماجرا انواع LOW POWER WAN ها وجود دارند که برای کاربران نهایی یعنی مشتریان بسیار مفیدتر و کاربردی تر هستند به این صورت که رایگان برای آنان عرضه می‌شود. این زیرساخت تکنولوژی اینترنت اشیا دارای سخت افزار ارزان تری نسبت به شبکه های سلولی است و به مخاطبان خود این اجازه را می‌دهد که کاربر نهایی سفارشی سازی بیشتری داشته باشد.

شبکه اینترنت اشیا مبتنی بر شبکه ی سلولی
شبکه های تشکیل دهنده زیرساخت اینترنت اشیا
شبکه های تشکیل دهنده زیرساخت اینترنت اشیا

دو نوع اتصال اصلی برای IOT مبتنی بر راه ارتباطی شبکه های سلولی وجود دارد، در ادامه این دو راه ارتباطی را می‌توانید مشاهده کنید:

اینترنت اشیا باند باریک (NB-IOT)
اینترنت اشیا ۱M (CAT-M۱)
این دو راه ارتباطی بالا هر دو مبتنی بر شبکه های سلولی هستند. البته در بین این دو تفاوتی وجود دارد به این صورت که NB-IOT با پهنای باند بسیار کوچک تر که باعث می‌شود، قدرت کمتری داشته باشد در مقابل ۱M با پهنای باند بیشتر توانی برای رقابت نداشته باشد.

خوشبختانه هر دو راه ارتباطی دارای برد بسیار طولانی هستند که به نظر خوب می‌رسد. NB-IOT حتی قادر به پوشش بردی به اندازه ی ۱۰۰ کیلومتر است. خوشبختانه با توجه به استانداردهای این دو نوع ارتباطی و مورد تایید بودن آن‌ها به راحتی می‌توانید به سخت افزارهای آن دسترسی داشته باشید و آن‌ها را خرید کنید و یا قطعات معیوب را تعویض نمایید. این مزیت بزرگ شبکه های سلولی در مقابل LPWAN است که پیشتر به آن اشاره کردیم. طول عمر دستگاه های مبتنی بر شبکه های سلولی به نسبت بیشتر است و شما اطمینان بیشتری بر این شبکه ارتباطی می‌توانید داشته باشید. این مزیت ها باعث شده است که راه های ارتباطی مبتنی بر شبکه های سلولی از راه های ارتباطی شبکه های LPWAN طرفداران بیشتری داشته باشد.

****

اینترنت اشیا (IoT) به ارتباطات معتبری برای ایجاد شبکه‌ها و به اشتراک‌گذاری داده‌ها نیاز دارد. با توجه به طیف گسترده‌ای از موارد استفاده، برنامه‌ها و الزامات، طیف وسیعی از فناوری‌های ارتباطی نیز وجود دارند که اپراتورها، توسعه دهندگان و شرکت‌ها / مشتریان می‌توانند انتخاب کنند. درک ویژگی‌های مختلف گزینه‌های ارتباطات ضروری است. در ادامه در مورد برخی از مهمترین جزئیات گزینه‌های بی‌سیم IoT مورد بررسی قرار می‌گیرد.

شبکه‌های بنیادین

فناوری‌های ارتباطی IoT به‌طور گسترده‌ای به دو دسته شبکه‌های سلولی و شبکه‌های LPWAN بدون مجوز تقسیم می‌شوند. تکنولوژی شبکه‌های سلولی IoT ، اعتبار خود را از طریق زیرساخت‌های نسبتاً سازگار و استاندارد شده تضمین می‌کند. آنها عموماً از داده‌های بزرگتر، عمر باتری کمتر و سخت‌افزار ارزان‌تر پشتیبانی می‌کنند. در نتیجه، راهکارهای IoT مبتنی شبکه‌های سلولی به‌طورکلی توسط اپراتورهای بزرگ و دسترسی به طیف مجاز و طرح‌های سخت‌افزاری ارائه شده است.

انواع LPWAN وجود دارد که در طیف بدون مجوز (رایگان برای همه کاربران) عمل می‌کنند که به نفع کاربران نهایی است. این تکنولوژی‌ها دارای سخت‌افزار ارزان‌تر هستند و اجازه می‌دهند کاربر نهایی سفارشی‌سازی بیشتری داشته باشد.

IoT مبتنی بر شبکه‌ی سلولی

دو نوع اتصال اصلی IoT سلولی وجود دارد: IoT باند باریک (NB-IoT) و (IoT رده‌ی ۱M Cat-M)۱ . هر دو مبتنی بر استانداردهای شبکه‌ی سلولی هستند، با ای تفاوت که NB-IoT پهنای باند بسیار کوچکتر و در نتیجه قدرت انتقال کمتری از Cat-M۱ دارد.
هر دو فناوری IoT سلولی دارای برد بسیار طولانی هستند. NB-IoT از لحاظ تئوری قادر به پوشش محدوده تا ۱۰۰ کیلومتر است. استفاده از استانداردهای جهانی شبکه‌های سلولی به این معنی است که سخت‌افزار آن‌ها به آسانی عرضه می‌شود، طول عمر دستگاه بیشتر است و اطمینان بیشتری توسط اپراتورهای شبکه در مقایسه با LPWAN بدون مجوز تضمین می‌شود.

برای اکثر برنامه‌های IoT، NB-IoT ارجحیت بیشتری از Cat-M۱ دارد. نرخ داده‌های ارائه شده توسط Cat-M۱ غیرضروری است و ممکن است هزینه‌های بیشتری را تحمیل کند. بااین‌حال، Cat-M۱ پشتیبانی از تحرک را فراهم می‌کند، به این معنی که بیشتر برای شبکه‌های بزرگ با گره‌های پویا مثل حمل و نقل و سناریوهای کنترل ترافیک مناسب است. Cat-M۱ همچنین امکان انتقال داده‌های صوتی را فراهم می‌آورد که یک مزیت عمده برای اپلیکیشن‌های مانند پاسخ اضطراری است.

سخت‌افزار مبتنی بر شبکه‌ی سلولی IoT (یعنی ماژول مورد استفاده برای اتصال یک دستگاه به شبکه وسیع‌تر) نسبت به LPWAN (حدود ۱۰ دلار برای هر ماژول در مقابل ۲ دلار) گرانتر می‌شود علاوه بر این، به دلیل اینکه آنها می‌توانند در زیرساخت‌های سلولی قرار گیرند، پوشش تلفن همراه موجود می‌تواند به اپلیکیشن‌های IoT امکان دسترسی سریع و بدون نیاز به استفاده از نقاط دسترسی اختصاصی را بدهد.

LPWAN بدون مجوز

LPWAN های بدون مجوز به‌طور خاص برای شبکه‌های سفارشی IoT با تأکید بر نرخ داده کم، عمر باتری، و پوشش طولانی / گسترده طراحی شده‌اند. آنها مشابه با وای‌فای در مقیاس بزرگتر هستند. دو نوع اصلی از LPWAN بدون مجوز LoRa و SigFox هستند. هر دو از شرکت‌های فرانسوی ساخته شده‌اند و به‌طور خاص برای دستگاه‌های با برد وسیع، سرعت کم و عمر باتری طولانی طراحی شده‌اند. محدوده پوشش دهی آن‌ها می‌تواند تا ۱۰ کیلومتر یا بیشتر باشد. در مقایسه با گزینه‌های شبکه‌های سلولی، هزینه‌های اتصال دستگاه برای این گونه‌ها به‌طورکلی ارزان‌تر است (حدود ۲ دلار برای هر ماژول، گاهی کمتر)، و آنها را برای برنامه‌های محلی و یا در مقیاس کوچک جذاب‌تر می‌سازند.

استفاده از IoT برای صنایع مختلف که همه آنها از لحاظ عمر باتری، محدوده، داده‌ها و هزینه‌ها متفاوت است، به این معنی است که برخی از فناوری‌های اتصال IoT برای صنایع خاص مناسب‌تر از دیگران هستند.

سایر گزینه‌های موجود برای شبکه‌های IoT

چندین شبکه‌ی دیگر برای دستگاه‌های موجود وجود دارد، بعضی از آنها که قبلاً کارایی خود را ثابت کرده‌اند، برای برنامه‌های موجود استفاده می‌شوند. Wi-Fi، بلوتوث، NFC، ZigBee و ماهواره از جمله تکنولوژی‌های بی‌سیم رایج هستند که لوازم روزمره مانند سیستم‌های سرگرمی خانگی، دستگاه‌های پزشکی، گوشی‌های هوشمند و درب بازکن‌ها را به یکدیگر مرتبط می‌کنند. یک سیستم IoT واقعی ترکیبی کارآمد از فناوری‌های مختلف شبکه‌های اتصال را با استفاده از ابزارهای مختلف برای حل مشکلات خاص در یک شبکه ترکیبی، شامل می‌شود.

شبکه های حسگر بی سیمWSN

معرفی شبکه های حسگر بی سیم

شبکه های حسگر بی سیم شامل تعداد زیادی نود حسگر می باشند که در یک محیط پراکنده شده اند. این نوع از شبکه، وسیله مناسبی برای جمع آوری و ارسال اطلاعات محیطی و یا اطلاع رسانی وقوع یک رخداد ، به یک نود مرکزی می باشد. این شبکه ها دارای ویژگی ها و خصوصیات و محدودیتهای مربوط به خود می باشند که موجب متمایز شدن شبکه های حسگر از سایر شبکه ها شده است.

یک شبکه حسگر متشکل از تعداد زیادی نودهای حسگر است که در یک محیط به طور گسترده پخش شده اند و به جمع‌آوری اطلاعات از محیط می پردازند. لزوماً مکان قرار گرفتن نودهای حسگر، از قبل تعیین شده و مشخص نیست. چنین خصوصیتی این امکان را فراهم می آورد که بتوانیم آنها را در مکان‌های خطرناک و یا غیرقابل دسترس رها کنیم.

از طرف دیگر این بدان معنی است که پروتکل‌ها و الگوریتم‌های شبکه‌های حسگر باید دارای توانایی خود ساماندهی باشند. دیگر خصوصیت‌های منحصر به فرد شبکه‌های حسگر، توانایی همکاری و هماهنگی بین نودهای حسگر است.

اجزا شبکه های حسگر بی سیم :

هر نود حسگر روی بورد خود دارای یک پردازشگر است و به جای فرستادن تمامی اطلاعات خام به مرکز یا به نودی که مسئول پردازش و نتیجه‌گیری اطلاعات است، ابتدا خود یک سری پردازش‌های اولیه و ساده را روی اطلاعاتی که به دست آورده است، انجام می دهد و سپس داده‌های نیمه پردازش شده را ارسال می کند.

کاربردهای شبکه حسگر

یک شبکه حسگر بی‌سیم، کاربردهای مهمی دارد. ازجمله می توان به مانیتورینگ راه دور محیط، و ردگیری هدف اشاره نمود. دسترس پذیری حسگرهای بی سیم بخصوص در سال های اخیر که حسگرها کوچکتر، ارزانتر، و هوشمندتر، این قابلیت ها را امکانپذیر می سازد. این حسگرها مجهز به واسطه های بی سیمی هستند که ارتباط حسگرها با هم و تشکیل شبکه را امکانپذیر می سازد. طراحی یک شبکه حسگر بی سیم، درحد قابل توجهی به کاربرد، وابسته است و فاکتورهایی مثل محیط، اهداف طراحی آن محیط، هزینه، سخت افزار، و محدودیت های سیستمی، باید لحاظ شوند.

کاربردهای WSN را می توان به دو مجموعه تقسیم نمود:

- نظارت/مانیتورینگ(Monitoring)
- پیگیری/ردگیری(Tracing)

۱- کاربردهای نظارت شامل نظارت محیط بسته/ فضای آزاد، نظارت بر خوبی و سلامتی، نظارت بر نیرو، نظارت بر مکان دارایی، اتوماتیک سازی پردازش و تولید، و نظارت ساختاری و لرزشی است.
۲- کاربرد های پیگیری شامل پیگیری اشیاء، حیوانات، انسان ها، و خودروها می باشد.

WSNها دارای پتانسیل زیادی برای کاربردهایی مانند موارد زیر دارند:

- تعقیب و نظارت بر اشیای نظامی
- امداد بلایای طبیعی
- نظارت سلامتی بیوداروبی
- لرزه نگاری و اکتشاف محیط های حادثه خیز

یک WSN در تعقیب و نظارت بر اشیای نظامی، می توان برای تشخیص و شناسایی متجاوزین استفاده نمود. از مثال های خاص می توان همبستگی-فضایی و حرکت های هماهنگ نیروها و تانک را نام برد. در بلایای طبیعی، گره های حسگری می توانند محیط را حس و بلایا را قبل از وقوعشان تشخیص دهند. در کاربردهای بیومدیکال، جراحی های کاشت حسگرها می تواند در تحت نظر گرفتن سلامتی بیمار کمک کند. برای حس لرزش، با پخش کردن حسگرها در نواحی آتشفشانی می توان وضعیت زمین لرزه ها و فوران ها را تشخیص داد.

طراحی شبکه های حسگر بیسیم

برخلاف شبکه های رایج، یک WSN طراحی ها و محدودیت های منابع خود را دارد.

۱- محدودیت منابع شامل **مقدار محدود انرژی، دامنه کوتاه ارتباطی، پهنای باند کم، و پردازش و ذخیره سازی محدود در گره ها** است .
۲- محدودیت های طراحی، وابسته به کاربرد و محیطی است که نظارت خواهد شد .محیط، نقش کلیدی در تعیین اندازه شبکه، نحوه توزیع گره ها، و توپولوژی شبکه دارد. اندازه شبکه، نسبت به محیط تحت نظر گرفته شده متغیر است. برای محیط های بسته، تعداد گره های کمی برای تشکیل شبکه در فضاهای محدود لازم است در حالی که ممکن است فضاهای آزاد، به تعداد گره های بیشتری برای پوشش ناحیه بزرگتر نیاز داشته باشند. هنگامی که محیط برای انسان غیرقابل دسترس باشد یا شبکه شامل صدها تا هزاران گره باشد،

یک **پخش اقتضایی** نسبت به **پخش طرح ریزی شده**، ارجحیت دارد. موانع موجود در محیط نیز می توانند ارتباط میان گره ها را محدود نمایند که در واقع روی همبندی شبکه (یا توپولوژی) تاثیر می گذارند.

شبکه های Ad-hoc به شبکه های آنی و یا موقت گفته می شود که برای یک منظور خاص به وجود می آیند. در واقع شبکه های بی سیم هستند که گره های آن متحرک می باشند. تفاوت عمده شبکه های Ad-hoc با شبکه های معمول بی سیم ۸۰۲,۱۱ در این است که در شبکه های Ad-hoc مجموعه ای از گره های متحرک بی سیم بدون هیچ زیرساختار مرکزی نقطه دسترسی و یا ایستگاه پایه برای ارسال اطلاعات بی سیم در بازه ای مشخص به یکدیگر وصل می شوند.
ارسال بسته های اطلاعاتی در شبکه های بی سیم Ad-hoc توسط گره های مسیری که قبلا توسط یکی از الگوریتمهای مسیریابی مشخص شده است، صورت می گیرد. نکته قابل توجه این است که هر گره تنها با گره هایی در ارتباط است که در شعاع رادیویی اش هستند، که اصطلاحا گره های همسایه

نامیده می شوند.

پروتکلهای مسیریابی بر اساس پارامترهای کانال مانند تضعیف انتشار چند مسیره، تداخل و همچنین بسته به کاربرد شبکه به صورت بهینه طراحی شده اند. در هنگام طراحی این پروتکلها به امر تضمین امنیت در شبکه های Ad-hoc توجه نشد. در سالهای اخیر با توجه به کاربردهای حساس این شبکه از جمله در عملیاتهای نظامی، فوریتهای پزشکی و یا مجامع و کنفرانسها، که نیاز به تامین امنیت در این شبکه ها بارزتر شده است، محققان برای تامین امنیت در دو حیطه عملکرد و اعتبار پیشنهادات گوناگونی را مطرح کردند و می کنند.

مسائل کلیدی شبکه حسگر

این که گره های حسگر، **قابلیت خود–سازماندهی** داشته باشند، از دید نیازمندی های کاربرد و مدیریت شبکه، مهم است. در این حالت، گره های حسگر این قابلیت را دارند که خودشان را داخل یک شبکه سازماندهی کرده و متعاقبا بصورت کارآمدی، قادر به کنترل و مدیریت خود باشند. چون گره های حسگری از لحاظ انرژی، ظرفیت پردازشی، و ذخیره سازی محدود هستند، پروتکل های ارتباطی و سرویس های مدیریتی جدید برای برآوردن این نیازمندی ها، لازم خواهد بود.

پروتکل ارتباطی شامل ۵ لایه استاندارد برای لایه های پروتکل است که عبارتند از:

- لایه کاربرد
- لایه انتقال
- لایه شبکه
- لایه انتقال داده
- لایه فیزیکی

پروتکل ها در لایه های مختلف در برابر دینامیک شبکه و کارایی انرژی پاسخگو هستند. خدماتی همچون **مکانیابی، پوشش، ذخیره سازی، همگام سازی، امنیت، و تجمیع و فشرده سازی داده ها** به عنوان **سرویس های شبکه حسگر** بررسی شده اند.

پیاده سازی پروتکل های لایه های مختلف از پشته پروتکل **شبکه حسگر بی سیم** ، می تواند بطور موثری روی **مصرف انرژی، تاخیر انتها به انتها**، و کارایی سیستم تاثیر گذارد. بهینه سازی ارتباط و **حداقل کردن مصرف انرژی مهم** است .پروتکل های شبکه ای رایج به خاطر اینکه طراحی آنها متناسب با نیازمندی های شبکه های WSN نیست، بنابراین به خوبی با آن کار نمی کنند. از این رو، پروتکل های کارا از لحاظ انرژی برای تمام این لایه های پشته پروتکل پیشنهاد شده است. این پروتکل ها از بهینه سازی های بین–لایه ای با پشتیبانی از تعامل بین لایه های پروتکل بهره جسته اند. خصوصا، اطلاعات مربوط به وضعیت پروتکل یک لایه برای تامین نیازمندی های خاصWSN ، میان لایه های دیگر به اشتراک گذاشته شده است.

چون گره های حسگری روی **انرژی باتری** محدود عمل می کند، مصرف انرژی نگرانی بسیار مهمی در یک WSN می باشد و تحقیقات قابل توجهی روی بدست آوردن و کمینه کردن مصرف انرژی تمرکز دارد. زمانی که انرژی یک گره حسگر تمام شد، می میرد و از شبکه جدا می شود که می تواند تاثیر قابل توجهی روی عملکردبرنام کاربردی بگذارد. طول عمر شبکه حسگر بستگی به تعداد گره های فعال و همبندی شبکه دارد، بنابراین برای **بیشینه کردن طول عمر شبکه**، انرژی باید به صورت کارا مصرف شود. بدست آوردن انرژی توسط گره مستلزم کسب انرژی از یک منبع انرژی است.

منابع بالقوه انرژی عبارتند از:

- سلول های خورشیدی
- ارتعاش
- سلول های تقویتی
- پارازیت های صوتی
- منبع تغذیه سیار

در رابطه با کسب انرژی از محیط، تکنیک کامل فعلی سلول های خورشیدی هستند که از نور انرژی تولید می کنند. همچنین کارهایی برای استفاده از منبع انرژی سیار مانند ربات نیز برای تجدید انرژی گره ها انجام یافته است. در این سناریو، ربات ها باید مسئول شارژ خودشان و تحویل انرژی به گره ها می باشند.

صرفه جویی مصرف انرژی در یک WSN طول عمر شبکه را بیشینه کرده و از طریق ارتباطات بی سیم مطمئن و کارآمد، جایگیری هوشمندانه حسگر برای رسیدن به پوششی مناسب، مدیریت کارآمد و مطمئن حافظه ذخیره سازی، و تجمیع و فشرده سازی کامل داده ها، قابل دستیابی است.

روش های فوق، سعی در ارضای هر دوی محدودیت های انرژی و ارائه **کیفیت سرویس** (QOS) برای کاربرد را دارند.

برای ارتباطات مطمئن، سرویس هایی مانند **کنترل ازدحام، نظارت فعال بافر**(AQM) ، تصدیق(acknowledgment) ، و **بازیابی بسته های گم** شده برای گارانتی تحویل مطمئن بسته، ضروری می باشند.

قدرت ارتباط وابسته به محل قرار گیری گره های حسگر می باشد. جایگیری پراکنده و خلوت حسگر باعث انتقال فاصله–طولانی و مصرف انرژی بیشتر خواهد شد در حالی که جاگیری متراکم حسگر باعث انتقال فاصله–کوتاه و مصرف کمتر انرژی خواهد شد. پوشش با جایگیری حسگرها ارتباط دارد. مجموع تعداد حسگرها در شبکه و جاگیری آنها، درجه پوشش شبکه را مشخص خواهند نمود. بسته به کاربرد، ممکن است برای بالا بردن دقت داده های حس شده، به درجه بالایی از پوشش نیاز داشته باشیم. در این تحقیق، پروتکل ها و الگوریتم های جدید توسعه یافته در این زمینه را بازبینی خواهیم نمود.

انواع شبکه حسگر

شبکه های حسگر بی سیم از لحاظ ساختارمندی به دو گروه قابل طبقه بندی است:

- ساختارمند
- بدون ساختار

یک WSN بدون ساختار نوعی است که شامل مجموعه انبوهی از گره های حسگر است. ممکن است گره های حسگر به صورت یک شبکه اقتضایی در یک حوزه پخش شوند .یک بار که گره ها پخش شدند، شبکه به حال خود رها می شود تا وظایف و عملیات نظارت و گزارش را انجام دهد. در یک WSNبدون ساختار، نگهداری شبکه مانند مدیریت اتصالات و کشف عیب ها سخت است چون تعداد گره ها زیاد است.

در یک WSN ساختارمند، بخش یا تمام گره های حسگری با نقشه قبلی پخش می شوند. مزیت یک شبکه ساختارمند این است که می توان گره های کمتری پخش نمود و در نتیجه نیاز به نگهداری کمتر و هزینه مدیریتی کمتری خواهد داشت. به این خاطر گره های کمتری می توان پخش نمود که گره ها برای پوشش دادن ناحیه در نقاط خاصی قرار می گیرند ولی در پخش به صورت اقتضایی ممکن است نواحی پوشش داده نشده وجود داشته باشد.

WSNهای فعلی در روی زمین، زیر زمین و در زیر آب پخش می شوند. یک شبکه حسگر برحسب محیط، با چالش ها و محدودیت هایی روبرو است. پنج نوع WSN وجود دارد که عبارتند از:

- WSNزمینی
- WSNزیرزمینی
- WSNزیرآبی
- WSNچند رسانه ای
- WSNمتحرک

WSNهای زمینی

معمولا شامل صدها تا هزاران گره حسگر بی سیم ارزان است که به یکی از انواع، اقتضایی یا از قبل مشخص شده در منطقه مورد نظر پخش شده است. در پخش به صورت اقتضایی، گره های حسگر می توانند توسط هواپیما پخش شده و به صورت تصادفی در منطقه هدف جای گیرند.

در پخش به صورت از قبل طرح ریزی شده، مدلهای جایگذاری شبکه ای، جایگذاری بهینه، و جایگذاری دوبعدی و سه بعدی وجود دارند. در یک WSNزمینی، ارتباط امن در یک محیط متراکم حائز اهمیت است. گره های حسگری زمینی باید بطور موثر قادر به ارسال داده ها به ایستگاه پایه باشند. با آنکه انرژی باطری محدود است و ممکن است قابل شارژ مجدد نباشد، اما ممکن است گره های حسگر مجهز به منبع نیروی ثانوی مانند سلول های خورشیدی باشند. در هر مورد، حفظ انرژی برای گره های حسگری مهم است. برای یک WSN زمینی، می توان با مسیریابی بهینه چند–گامی، فاصله انتقال کوتاه، تجمیع داده داخل–شبکه، حذف افزونگی داده ها، کمینه کردن تاخیرات، و بهره گیری از عملیات هایی با duty-cycle کم، انرژی را حفظ نمود.

WSNهای زیرزمینی

شامل تعدادی گره حسگری مدفون زیر خاک، غار و یا معدن است که برای نظارت بر شرایط زیرزمینی استفاده می شود. گره های چاهک دیگری در بالای زمین برای انتقال اطلاعات از گره ها به ایستگاه پایه قرار می گیرند. یک WSN زیرزمینی به دلیل تجهیزات، پخش و نگهداری، نسبت به WSN زمینی بسیار گرانتر است. گره های حسگری زیرزمینی بدین دلیل گران هستند که باید اجزای مناسبی برای اطمینان از ارتباط مطمئن از طریق خاک، صخره ها، آب و دیگر مواد معدنی، در آنها استفاده شود. محیط زیرزمینی ارتباطات بی سیم را به خاطر تلفات و سطوح بالای تضعیف سیگنال، با چالش جدی مواجه می کند. برخلاف WSN های زمینی، پخش یک WSN زیرزمینی نیازمند طرح و نقشه دقیق، انرژی و وقت است. انرژی مقوله ای مهم در WSN های زیرزمینی می باشد. گره های حسگر زیرزمینی همانند WSN زمینی حاوی نیروی باطری محدود بوده و بعد از پخش آنها در زمین، شارژ یا تعویض

باطریشان بسیار سخت خواهد بود. همانند قبل، حفظ انرژی برای افزایش طول عمر شبکه، موضوع کلیدی است که با پیاده سازی پروتکل های ارتباطی کارآمد، قابل دستیابی خواهد بود.

WSNهای زیرآبی

شامل تعدادی گره های حسگر و خودروهای پخش شده زیر آب می باشند. برخلاف WSNهای زمینی، گره های حسگر زیرآبی بسیار گران بوده و تعداد کمتری از این گره های حسگر زیر آب پخش می شوند. خودروهای خودمختار زیرآبی برای اکتشاف یا جمع آوری داه ها از گره های حسگر استفاده می شوند. در مقایسه با پخش انبوه گره های حسگر در یک WSN زمینی، پخش خلوتی از گره های حسگر در زیر آب اتفاق می افتد. معمولا ارتباطات بی سیم زیر آبی از طریق انتقال امواج صوتی برقرار می گردد. یک چالش در ارتباط صوتی زیر آب پهنای باند محدود، تاخیر انتشار زیاد، و مسئله محو شدن سیگنال است. چالش دیگر خرابی گره های حسگر بدلیل شرایط محیطی است. گره های حسگر زیر آبی باید توانایی خود–پیکره بندی و سازگاری با محیط خشن اقیانوس را داشته باشند. گره های حسگر زیرآبی مجهز به باطری محدودی است که قابل تعویض یا شارژ نیست. حل مسئله حفظ انرژی در WSNهای زیرآبی مستلزم توسعه ارتباطات و تکنیک های شبکه ای موثر زیرآبی است.

WSNهای چند رسانه ای

برای ارائه امکان نظارت و پیگیری وقایع در شکل چند–رسانه ای مانند ویدئو، صدا و تصویر است WSN.های چند رسانه ای شامل تعدادی گره حسگر ارزان مجهز به دوربین و میکروفن است. این گره های حسگر برای بازیابی، پردازش، همبستگی، و فشرده سازی داده ها، از طریق یک اتصال بی سیم به هم مرتبط هستند. گره های حسگر چند–رسانه ای برای ضمانت پوشش، بر اساس طرح از پیش تعیین شده در محیط پخش می شوند. چالش های پیش روی WSN چند–رسانه ای عبارتند از پهنای باند مورد نیاز بالا، مصرف انرژی زیاد، تامین کیفیت سرویس(QOS) ، تکنیک های پردازش و فشرده سازی داده، و طراحی میان–لایه ای. محتوای چند–رسانه ای مانند جریان ویدیو برای تحویل محتوا نیازمند پهنای باند بالایی است. ارائه QOS بدلیل تاخیر های متغیر و ظرفیت کانال متغیر، یک مبحث چالش برانگیز در WSN های چند–رسانه ای است. رسیدن به یک سطح مشخص از QOS برای تحویل مطمئن محتوا ضروری است. پردازش، فیلترینگ، و فشرده سازی داخل شبکه ای بطور موثری کارایی شبکه را با فیلتر کردن و استخراج اطلاعات تکراری و زائد و ادغام محتویات، بهبود می بخشد. بطور مشابه، تعامل بین لایه ای میان لایه های مختلف می تواند پروسه تحویل و پردازش را بهبود بخشد.

WSNهای متحرک

شامل مجموعه ای از گره های حسگر است که توانایی حرکت و تعامل با محیط فیزیکی را دارند. گره های سیار مانند گره های ثابت، قادر به حس، محاسبه و ارتباط هستند. تفاوت کلیدی گره های سیار، توانایی آنها برای تغییر موقعیت و موضع گیری مناسب در شبکه است. یک WSN می تواند با یک پخش اولیه شروع شود، سپس گره ها می توانند برای جمع آوری اطلاعات پخش شوند. اطلاعات جمع آوری شده توسط یک گره سیار می تواند هنگامی که دو گره سیار در بازه ارتباطی همدیگر قرار دارند، مبادله شود. تفاوت اساسی دیگر پخش داده می باشد. در یک WSNایستا، داده می توانند با یک مسیریابی ثابت و یا سیل آسا پخش شود، در حالی که در WSN های سیار از مسیریابی پویا استفاده می شود. چالش ها در WSN سیار عبارتند از پخش، مکانیابی، خود–سازماندهی، مسیریابی و کنترل، پوشش، انرژِی، نگهداری، و پردازش داده. کاربردهای WSN سیار عبارتند از نظارت بر محیط، پیگیری

اهداف، جستجو و نجات، و نظارت real-time مواد پرخطر، اما کاربرد ها به این موارد محدود نمی شود. برای نظارت محیطی بر مناطق پرخطر (حادثه خیز)، که ممکن است پخش دستی در آن امکانپذیر نباشد. گره های حسگر سیار می توانند بعد از پخش شدن، برای ارائه پوشش مورد نیاز به نواحی رخداد ها حرکت کنند. گره های حسگر سیار در نظارت و پیگیری نظامی، می توانند بر حسب هدف با هم همکاری و تصمیم گیری نمایند. گره های حسگر سیار در مقایسه با گره های حسگر ثابت، می توانند به درجه بالاتری از پوشش و همبندی دست یابند. هنگام وجود موانع در میدان، گره های حسگر سیار می توانند plan ahead و بطور مناسب به نواحی مناسب حرکت کنند تا اهداف بهتر در تیررسشان قرار گیرد.

سیستم داخلی حسگر

برای اینکه یک حسگر بتواند در یک شبکه حسگر بی سیم کار کند، لازم است چندین مسئله مربوط به سیستم داخلی، به کمک پلتفورم سیستم و پشتیبانی از سیستم عامل (OS) حل شود. علاوه بر آن، استانداردهای پشتیبانی شده، ذخیره سازی و testbed های فیزیکی در زیرقسمت هایی که در ادامه آمده، مورد مطالعه قرار گرفته است.

پلتفورم WSN های حاضر برای پشتیبانی محدوده وسیعی از حسگرها ساخته شده اند. محصولاتی که حسگر و گره های حسگر عرضه می کنند، شامل اجزای مختلف رادیویی، پردازنده ها، و ذخیره سازی است.مجتمع نمودن چندین حسگر در یک پلتفرم WSN بخاطر متفاوت بودن سخت افزار حسگر و مشکل ساز بودن پردازش داده های خام با استفاده از منابع محدود گره های حسگر، یک چالش است. نرم افزار سیستمی، مانند سیستم عامل باید طوری طراحی شود که از این زیرساخت های حسگر، پشتیبانی کند. تحقیقات در این زمینه شامل طراحی زیرساخت هایی است که از مدیریت خودکار، بهینه سازی طول عمر شبکه، و برنامه ریزی توزیع شده پشتیبانی نماید.

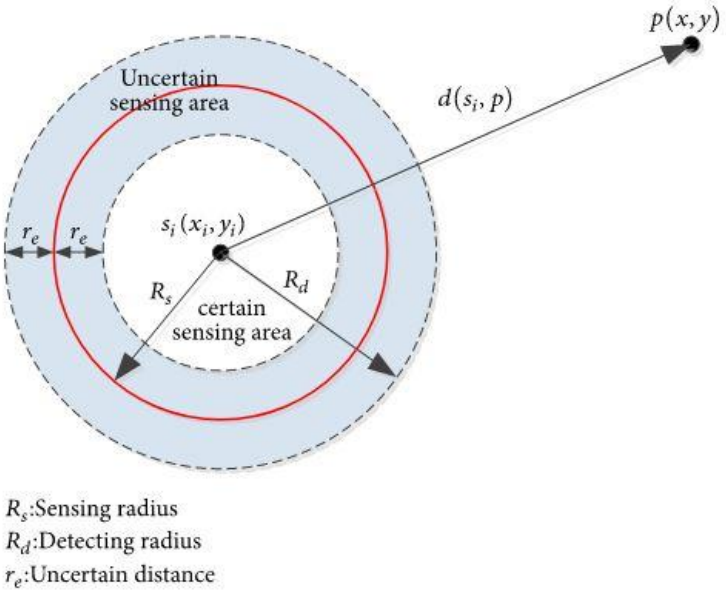
استانداردهای شبکه حسگر بی سیم با توجه به این مسئله توسعه یافته اند که نیاز اصلی در آنها، طراحی است که به کاهش مصرف منجر شود. یک استاندارد، عملکردها و پروتکل‌های لازم برای رویارویی گره‌های حسگر با شبکه‌های مختلف را تعریف می‌کند. برخی از این استانداردها عبارتند از:

- IEEE ۸۰۲,۱۵,۴
- ZigBee
- WirelessHART
- ISA ۱۰۰,۱۱
- IETF ۶LoWPAN
- IEEE ۸۰۲,۱۵,۳
- Wibree

شعاع حسگری گره

هر گره حسگر بیسیم در شبکه WSN یک شعاع حسگری (Sensing Radius) دارد .اگر شعاع حسگری یک گره حسگر را Rs بنامیم، یک دایره با شعاع Rs را می توان دور یک گره حسگر تصور کرد. ناحیه داخل این دایره فرضی همان ناحیه حسگری گره بوده و گره حسگر فقط قادر به حس

رویدادهای داخل ناحیه حسگری خود می باشد .یکی دیگر از مشخصه های یک گره حسگر، برد تشخیص (Detecting Radius) گره است که اینجا با Rd نشان داده شده است.



سرویس های شبکه

سرویس های تأمین(privisioning) ، سرویس های مدیریتی و سرویس های کنترلی، برای هماهنگی و مدیریت گره های حسگر توسعه یافته است. آنها عملکرد کلی شبکه را، برحسب نیرو، توزیع وظیفه، و استفاده منابع، بهبود می دهند. تأمین ، منابعی مانند نیرو و پهنای باند را به منظور بیشینه کردن کارآیی، به طور مناسب تخصیص می دهد. مکانیابی و پوشش جزئی از تدارک هستند. در یکWSN ، پوشش باید تحت پوشش قرار گرفتن ناحیه تحت نظارت را با یک درجه اطمینان بالایی تضمین نماید. اهمیت پوشش بدلیل تاثیر آن روی تعداد حسگرهای پخش شده، جایگیری این حسگرها، همبندی و انرژی میباشد. مکانیابی پروسه ای است که یک گره حسگر سعی در تعیین موقعیت خود بعد از پخش شدن دارد. سرویس های مدیریت و کنترل بدلیل ارائه پشتیبانی از سرویس های میان افزار مانند امنیت، همگام سازی، فشرده سازی و تجمیع داده، بهینه سازی میان-لایه ای و ...، نقش کلیدی در WSNها بازی می کنند. در این قسمت، ما تأمین، کنترل، و مدیریت سرویس را بر اساس اهدافشان مورد بررسی قرار می دهیم. خلاصه مختصری از هر یک نیز در قسمت های زیر آمده است.

مکانیابی

در WSN ها، گره های حسگری که در محیط به صورت اقتضایی پخش شده اند، از مکان خود دانش قبلی ندارند. مسئله تعیین موقعیت گره مربوط به مکانیابی است .روش های موجود برای مکانیابی عبارتند از سیستم موقعیت یابی جهانی(GPS) ، گره های beacon (یا لنگر)، و مکانیابی مبتنی بر تقریب. یک راه حل ساده برای این مسئله، تجهیز گره های حسگری به یک گیرنده GPS است. به هر حال ممکن است سیستمهایی که برپایه GPS

هستند، هنگامی که حسگرها در یک محیط با موانعی مانند شاخ و برگ های انبوه پخش شده باشند، کار نکنند. روش beacon (لنگر)، از گره های beacon(لنگر) که موقعیت خود را می دانند، برای کمک به دیگر حسگرها برای تعیین موقعیت خود، بهره می گیرد. این روش نیز کمبود های خود را دارد. بطوری که در شبکه های بزرگ بخوبی توسعه نمی یابد و ممکن است مشکلاتی بخاطر شرایط محیطی بوجود آید. در مکانیابی بر پایه تقریب گره ها با بهره گیری از گره های همسایه مکان خود را مشخص می کنند، سپس به عنوان beaconبرای گره های دیگر عمل می کنند. برخی تکنیک های دیگر نیز برای مکان یابی وجود دارد که با روش های فوق الذکر تفاوت دارند.

همگام سازی

همگام سازی زمانی در شبکه حسگر بی سیم برای مسیریابی و حفظ نیرو مهم است. دقیق نبودن زمان می تواند به طور قابل ملاحظه ای طول عمر شبکه را کاهش دهد. همزمانی سراسری به گره ها امکان هماهنگی و انتقال داده به طریق زمانبندی شده خواهد داد. هنگامی که میزان تداخلات و باز–ارسال ها کم باشد، مصرف انرژی کاهش خواهد یافت. علاوه بر آن، زمانی که گره ها duty-cycledباشند، انرژی حفظ خواهد شد. هدف پروتکل های موجود همزمانی ، تقریب دقیق عدم قطعیت زمان و همگام سازی **ساعت محلی** هر گرهدر شبکه می باشد. گره های حسگر برای حفظ انرژی duty-cycled هستند. در سیکل–وظیفه، گره حسگر می تواند به صورت دوره ای رادیوی خود را برای حفظ انرژی خاموش و برای مشارکت در ارتباطات شبکه، روشن کند.

پوشش

مسئله تعیین پوشش حسگر برای یک ناحیه انتخاب شده(designated) ، هنگام ارزیابی اثربخشی(effectivness) شبکه حسگر بیسیم، اهمیت دارد. کیفیت نظارت در یک WSN بستگی به کاربرد دارد. کاربردهایی مانند پیگیری اهداف، نیازمند درجه بالایی از پوشش به منظور پیگیری دقیق اهداف هستند، در حالی که کاربردهایی مانند نظارت محیطی یا سکونتی می توانند درجه کمتری از پوشش را تحمل نمایند. درجه بالای پوشش، نیازمند نظارت همزمان چندین حسگر بر یک محل برای تولید نتایج مطمئن تر است. تحقیقات حاظر در زمینه پوشش روی حفظ انرژی متمرکز هستند.برخی از این تحقیقات تکنیک هایی را برای انتخاب مجموعه کمینه ای از گره های فعال برای بیدار ماندن و حفظ پوشش شبکه پیشنهاد داده اند .پیشنهاد بقیه تحقیقات، استراتژی های توزیع حسگر برای شناسایی توزیع شده در شبکه های مقیاس بالا میباشد.

فشرده سازی و تجمیع

فشرده سازی و تجمیع موجب کاهش هزینه ارتباطات و افزایش اطمینان انتقال داده ها می شود. فشرده سازی و تجمیع داده ها برای کاربردهایWSNای موثر هستند که مقدار داده زیادی برای ارسال درشبکه دارند. بسته به اهمیت داده ها، ممکن است یک روش، بهتر از روش های دیگر باشد. تکنیک های فشرده سازی داده مستلزم فشرده سازی اندازه داده ها قبل از ارسالشان می باشد. خارج نمودن از حالت فشرده در ایستگاه پایه انجام می گیرد. در فشرده سازی داده، از دست نرفتن اطلاعات و قابل بازیابی بودن تک به تک داده های خوانده شده (individual data readings are retained)مهم است. در تجمیع داده ها، داده ها از چندین حسگر جمع آوری شده و برای ارسال به ایستگاه مرکزی با هم ترکیب می شوند. در این حالت، داده های تجمیع شده بسیار پراهمیت تر از تک تکداده های خوانده شده خواهند بود. این روش اغلب در روش های مبتنی بر خوشه بندی استفاده می شود. هر یک از این تکنیک ها، یکی از مسائل انرژی، robustness، توسعه پذیری، دقت، و کارآیی را مدنظر قرار داده اند.

امنیت

یک WSN در مقابله تهدیدات و ریسک ها آسیب پذیر است. کارهایی که دشمن می تواند انجام دهد عبارتند از: تسخیر یک گره حسگر، دستکاری جامعیت داده، استراق سمع پیغام ها، تزریق پیغام های جعلی، و اتلاف منابع شبکه.

در اِعمال امنیت به یک شبکهWSN ،محدودیت هایی مانند محدود بودن فضای ذخیره سازی، ارتباطات، محاسبات، و قابلیت های پردازشی، وجود دارد. طراحی پروتکل های امن، نیازمند رعایت این محدودیت ها و دستیابی به کارایی قابل قبول بر اساس معیارهای امنیتی برای مرتفع نمودن نیازهای یک برنامه است.

پروتکل های ارتباطی

توسعه پشته پروتکل مطمئن و کارآمد از لحاظ انرژی برای پشتیبانی از کاربردهای مختلف WSN مهم است. بسته به کاربرد، ممکن است یک شبکه حسگر شامل صدها تا هزاران گره باشد. هر گره حسگر از پشته پروتکل برای ارتباط با دیگر گره ها و چاهک استفاده می کند. از این رو پشته پروتکل باید از لحاظ مصرف انرژی ارتباطی، کارآمد باشد و قادر به عملکرد کارآمد روی چندین گره حسگر باشد. در زیربخش های بعدی، مروری خواهیم داشت بر پروتکل های انرژی–کارآمد ارائه شده برای لایه انتقال، لایه شبکه، و لایه پیوند داده و تعاملات میان–لایه ای آنها.

لایه انتقال

لایه انتقال، تضمین کننده قابلیت اعتماد و کیفیت داده ها در منبع و چاهک می باشد. پروتکل های لایه انتقال در WSN ها باید از چند کاربردی (multiple application)، قابلیت اعتماد متغیر، بازیابی فقدان بسته، و مکانیزم کنترل ازدحام، پشتیبانی کنند. توسعه یک پروتکل لایه انتقال باید کلی و مستقل از کاربرد باشد. همچنین باید برای کاربردهای مختلف،"قابلیت اعتمادپکت" متفاوتی ارائه نماید. هر کاربردی در WSN می تواند سطح مختلفی از فقدان بسته را تحمل نماید. ممکن است فقدان بسته بخاطر ارتباطات رادیویی بد، ازدحام، تصادم بسته، پربودن حافظه، و خرابی گره باشد. هر گم شدن بسته ای می تواند انرژی را تلف کرده و کیفیت سرویس (QoS) را در تحویل داده کاهش دهد. تشخیص فقدان بسته و بازیابی صحیح بسته های گم شده می تواند بازدهی و مصرف انرژی را بهبود بخشد.

برای بازیابی بسته دو راه کار وجود دارد hop-by-hop :و انتها–به–انتها .باز– ارسال Hop-by-hop نیازمند این است که یک گره میانی اطلاعات بسته را در حافظه خود کش نماید. این روش از لحاظ انرژی کارآمدتر است زیرا فاصله باز–ارسال کوتاه تر است. در باز–ارسال انتها–به–انتها، منبع، تمام اطلاعات بسته را کش کرده و زمانی که یک بسته گم می شود، باز–ارسال را انجام می دهد .باز–ارسال انتها–به–انتها امکان داشتن قابلیت اطمینان متغیر را خواهد داشت در حالی که باز–ارسال hop-by-hop به خاطر فراهم آوردنقابلیت اطمینان بالاتر، عملکرد بهتری دارد.

مکانیزم کنترل ازدحام ، با نظارت و کشف ازدحام، باعث حفظ انرژی می شود .قبل از اینکه ازدحام رخ دهد، به منبع اطلاع داده می شود که نرخ ارسال را کاهش دهد. کنترل ازدحام، به کاهش دفعات باز–ارسال و جلوگیری از لبریز شدن بافر حسگر کمک خواهد کرد. در بازیابی بسته گم شده نیز دو روش برای کنترل ازدحام وجود دارد hop-by-hop :و انتها–به–انتها. در مکانیزم hop-by-hop هر گره ای در طول مسیر باید بر سرریزهای بافر نظارت کند. مکانیزم hop-by-hop ازدحام را با سرعت بیشتری نسبت به مکانیزم انتها–به–انتها یاد می گیرد .هنگامی که ازدحام توسط یک گره حسگر تشخیص داده شد، تمام گره ها در طول مسیر رفتار خود را تغییر خواهند داد. مکانیزم انتها–به–انتها برای تشخیص ازدحام به گره های انتهایی تکیه می کند. هنگامی که مهلت زمانی (timeout) به سر آید یا پاسخ های تکراری دریافت شود، نشانه ازدحام خواهد بود.برای بازیابی بسته گم شده و کنترل

ازدحام، سبک سنگینی میان روش های hop-by-hop و انتها-به-انتها وجود دارد. بسته به نوع، درجه اطمینان، و میزان حساسیت زمانی کاربرد، ممکن است یکی از روش ها بر دیگری برتری داشته باشد. پروتکل های لایه انتقال موجود در WSN ها سعی در پاسخ به مسائل طراحی فوق دارند.

لایه شبکه

لایه شبکه مسئول مسیریابی داده ها در طول شبکه از منبع به مقصد است .پروتکل های مسیریابی در WSN ها از چند جهت متفاوت از پروتکل های مسیریابی رایج هستند. اولا، گره های حسگر دارای آدرس های پروتکل اینترنت (IP) نیستند، بنابراین پروتکل های مبتنی بر IP-در WSN قابل استفاده نیستند .طراحی پروتکل های شبکه در یک WSN باید مقیاس پذیر)قابل توسعه (scalable – باشد. همچنین باید براحتی ارتباطات میان گره های زیادی را مدیریت کرده و داده های حسگر را به ایستگاه پایه منتقل نماید. محدودیت های منابع شبکه، مانند: انرژی، پهنای باند ارتباطی، حافظه، و قابلیت های محاسباتی محدود،بایددر پروتکل لحاظ شده باشد. با لحاظ شدن این محدودیت ها، طول عمر یک شبکه حسگر می تواند افزایش یابد. نهایتاً، پروتکل باید به مسائل کارآیی، تحمل خطا، عدالت، و امنیت پاسخگو باشد.

لایه انتقال داده

لایه پیوند داده به انتقال داده میان دو گره که یک اتصال مشترک مابین آنهاست، اشاره دارد. از آنجا که شبکه زیرین بی سیم است، برای انتقال موثر داده، نیاز به مدیریت و کنترل دسترسی به رسانه می باشد. طراحی پروتکل MAC باید شامل خصوصیاتی باشد که عبارتند از کارآیی انرژی، توسعه پذیری برای تراکم گره، همگام سازی فریم، عدالت، بهره وری پهنای باند، کنترل جریان، و کنترل خطا برای ارتباطات داده.

سرویس تشخیص و تصحیح خطا، علاوه بر لایه انتقال، در لایه پیوند داده نیز ارائه می شود. یکی از پر استفاده ترین تکنیک های تشخیص خطا،کنترل چرخشی افزونگی [۹۷] (CRC) است CRC .در WSN به صورتی که در ادامه می آید، عمل می کند. ابتدا فرستنده و گیرندهبایدقبل از انتقال، روی اندازه ی ثابتی از بلوک های داده، توافق نمایند. فرستنده بسته مربوط به لایه شبکه را به بلوک های داده، که در سمت گیرنده بازسازی خواهند شد، تقسیم می کند. می توان از یک CRCهشت بیتی برای تشخیص خطا استفاده نمود. بلوک های حاوی داده و بیت های CRCداخل یک فریم قرار می گیرند. هر فریم به دریافت کننده ارسال می شود. به محض دریافت فریم، گیرنده مشخص می کند که فریم دریافت شده دارای خطاست یا خیر. اگر فریم دارای خطا باشد، گیرنده پروسه بازیابی را برای استخراج این بلوک های خطادار، بعد از دریافت تعداد مشخصی فریم، شروع می کند.

تکنیک های بازیابی در WSN عبارتند از: تکرار خودکار درخواست(ARQ) ، ارسال تصحیح خطا(FEC) ، Hybrid ARQ (HARQ)، ترکیب ساده بسته(SPaC) ، و تنوع چند-رادیویی ARQ.(MRD) از اعلام وصول و مهلت زمانی برای بازخورد صریح بعنوان پاسخ به فرستنده استفاده می کند. بازخوردها می توانند به صورت اعلام وصول مثبت (ACK) یا اعلام وصول منفی (NACK) باشد. هنگامی که فرستنده NACK دریافت می کند یا مهلت زمانی تمام می شود، فریم داده را دوباره ارسال خواهد نمود. محدودیتی که برای ARQ وجود دارد، این است که محدود به تشخیص خطاهای فریم است. در صورتی که تنها یک بیت خطا هم داشته باشیم، کل فریم دوباره ارسال خواهد شد. در طرف دیگرFEC ، تعداد بازارسال ها را کاهش خواهد داد .فرستنده مقداری اطلاعات افزونه به هر پیغام اضافه می کند، بر این اساس، گیرنده می تواند خطاها را تشخیص و تصحیح نماید. مزیت FECکاهش باز-ارسال ها و حذف زمان انتظار برای ارسال اعلام وصول است Hybrid ARQ .نوعی از روش ARQ است که در آن هر دو روش ARQو FEC ترکیب شده اند. دو نوع شما برای Hybrid ARQ عبارتند از: نوع-۱ و نوع-۲/ نوع-۱ شامل بیت های تشخیص و تصحیح خطا در هر بسته ارسالی با استفاده از کد تصحیح است. نوع-۲ بیت های تشخیص خطا یا اطلاعات FEC را همراه داده انتقال می دهد. اگر خطایی در بسته اول تشخیص داده شد، منتظر بسته دوم خواهیم بود که شامل بخش های FEC و تشخیص خطا برای تصحیح خطا هستند. اگر خطا همچنان وجود دارد، بسته ها برای تصحیح خطا ترکیب خواهند شد SPaC .و MRD عمل تصحیح خطا را بوسیله ترکیب بسته های خراب و با استفاده از HARQ انجام می

دهند SPaC.بسته های خراب را در گیرنده بافر کرده و منتظر بازارسال می شود. فرستنده، علاوه بر باز–ارسال بسته اصلی، بیت های توازن را نیز ارسال می نماید. گیرنده به محض دریافت بسته باز–ارسال شده، عمل ترکیب بسته را برای استخراج خطاها انجام می دهد MRD .از دو تکنیک برای استخراج خطاها استفاده می کند. تکنیک اول ترکیب فریم با چندین فریم خطادار دیگر برای پرهیز از باز–ارسال فریم. تکنیک دوم طرح درخواست–برای–اعلام وصول برای بازیابی بسته است.

مسئله ای که در طراحی پروتکلMAC برای یک WSN وجود دارد، محدودیت هایی مانند انرژی، توپولوژی، و تغییرات شبکه می باشد. ، هدف اولیه پروتکلMAC ، کمینه کردن انرژی برای افزایش طول عمر شبکهمی باشد. یک پروتکلMAC باید حدالامکان از اتلاف انرژی بواسطه تصادم بسته ها، سربار، باز–ارسال بیش از اندازه، سربارهای کنترلی، و حالت بی کار (idle) جلوگیری نماید. همچنین باید با تغییرات توپولوژی وتغییرات شبکه، به طور کارآمدی سازگار باشد. برای دستیابی به بهره وری بالای کانال، اجتناب از تصادم، و کارآیی انرژی،طیف وسیعی از پروتکل های MAC پیشنهاد شده است.

لایه فیزیکی

لایه فیزیکی، واسطی برای انتقال جریان بیت ها روی رسانه ارتباطی فیزیکی ارائه می دهد. این لایه مسئول تعامل با لایهMAC ، انجام انتقال و دریافت، و مدولاسیون است. تعامل میان لایه فیزیکی و لایه MAC مسئله مهمی می باشد. در محیط بی سیم، نرخ خطا در لایه فیزیکی بالا و متغیر با زمان است. لایه MAC با لایه فیزیکی برای تشخیص و تصحیح خطا تعامل می کند. دیگر تعاملات شامل اشتراک اطلاعات کانال و انتقالات با لایهMAC ، به منظور رسیدن به کارآیی و بهره وری بالای منابع است.

برای یکWSN ، کمینه کردن مصرف انرژی و بیشینه کردن طول عمر شبکه از لایه فیزیکی شروع می شود. انرژی در لایه فیزیکی برای عملیات مدارات رادیویی و انتقال جریان بیت استفاده می شود.انرژی استفاده شده برای مدارات رادیویی ثابت است در حالی که ممکن است انرژی صرف شده برای انتقال داده برحسب channel loss، تداخل، و فاصله انتقال متغیر باشد. یک سبک–سنگینی میان انرژی انتقال و خطا وجود دارد. برای کمینه کردن اتلاف نیرو و عملکرد کارآمدتر شبکه، لازم است نیروی انتقال درست انتخاب شود. برای انتقال داده روی یک کانال بی سیم، نیاز به طرح های مدولاسیون داریم. برای رسیدن به بالاترین احتمال ممکن یک انتقال موفق تحت شرایط مختلف، طرح های مدولاسیون مختلفی توسعه داده شده است. طرح های مدولاسیون کارا از لحاظ انرژی باید هر دو انرژی مدار و انتقال را کمینه کنند. مطالعات اخیر تحقیقاتی عبارتند از نیازمندی های لایه فیزیکی، طراحی رادیو کم مصرف، طرح های انتقال آگاه از انرژی، و طرح های مدولاسیون.

لایه فیزیکی باید با درنظر گرفتن نیازمندی های WSN طراحی شود. منبع نیازمندی های لایه فیزیکی را با تمرکز روی ارتباطات دیجیتالی و تکنولوژی های موجود سخت افزاری بحث کرده است. اندازه ارتباطات دیجیتالی با رادیو به خاطر کوچک بودن گره های حسگر، می بایست کوچک باشد. همچنین به خاطر این امر که ممکن است صدها یا هزاران گره حسگر پخش شود، رادیو باید ارزان باشد .استفاده مجدد از رادیو برای حس و ارتباطات می تواند هزینه و انرژی را به مقدار قابل ملاحظه ای کاهش دهد. با لحاظ انرژی، رادیو باید کم مصرف باشد .فرضیات مهم باید زمانی که محل استفاده از سخت افزار تعیین شد، در نظر گرفته شود. اگر گره های حسگر به صورت انبوه پخش خواهند شد، احتمالا تداخل سیگنال امری غیرقابل اجتناب خواهد بود. هر گره حسگر می تواند نیروی انتقال را برای کاهش تداخلات کاهش دهد. به هر حال، نیاز به همگامی میان گره های حسگر وجود دارد. باید میان لینک و لایه های فیزیکی و همچنین میان گره های حسگر همگامی وجود داشته باشد. با همگام شدن می توان تداخلات ارتباطی را کمینه کرد. نهایتا اینکه

رادیوهایی با قابلیت چند پخشی برای انتقال همزمان داده به چندین گره حسگر مفید خواهند بود. در این حالت تنها گره های حسگر مورد نظر باید اطلاعات را دریافت کنند.

سه کلاس از تکنولوژی های لایه فیزیکی بر پایه پهنای باند در WSN ها عبارتند از narrow-band ،. spread-spectrum، و-ultra wideband. narrow-bandاز پهنای باند رادیویی که با نرخ سمبول کار می کند، استفاده می کند narrow-band .روی کارایی پهنای باند تمرکز دارد. کارایی پهنای باند معیار نرخ داده روی پهنای باند است. درspread-spectrum ، سیگنال باریک روی یک سیگنال پهن پخش می شود. در این حالت از تابع پخش برای مشخص کردن مستقل بودن پهنای باند از پیغام استفاده می شود spread-spectrum .قادر به کاهش انرژی مصرفی با حفظ ارتباطات موثر می باشد. همچنین در برابر تداخلات و اختلالات کانال های چند–مسیره پایدار است ultra-wideband .در مقابلspread-spectrum، از پهنای باند بیشتری، در محدوده گیگاهرتز، استفاده می کند ultra-wideband.سگنال های خود را روی پهنای باند بزرگی منتشر می کند بطوری که تداخل با دیگر رادیوها ناچیز خواهد بود ultra-wideband .همانند spread-spectrum می تواند با انرژی کمی ارتباط برقرار کند. مرجع [۶۶] نشان می دهد که تکنولوژی های spread-spectrum نیازمندی های WSN را بهتر از تکنولوژی narrow-band برآورده می کنند . narrow-bandکارایی پهنای باند را بهینه می کند در حالی که spread-spectrum و ultra-wideband یک سبک سنگینی میان پهنای باند و حفظ انرژی برقرار می کنند. سیستم های narrow-band نسبت به سیستم های spread-spectrumدر مقابل تداخلات، پایداری کمتری دارند. بسته به نوع spread-spectrum، همگامی می تواند مفید باشد و این بخاطر خصوصیات auto-correlationمربوط به دنباله شبه–تصادفی می باشد. سیستم های narrow-bandبرای انجام چند–پخشی طراحی نشده اند. در حالی که سیستم های spread-spectrumمی توانند با استفاده از کدهای شبه–تصادفی مناسب، به این امر دست یابند ultra-wideband .دارای خصوصیات جذاب زیادی است، اما در مقایسه با spread-spectrum چالش ها و مسائل فراوانی دارد. برای فهم بهتر ultra-widebandنیاز به مطالعات بیشتری است.

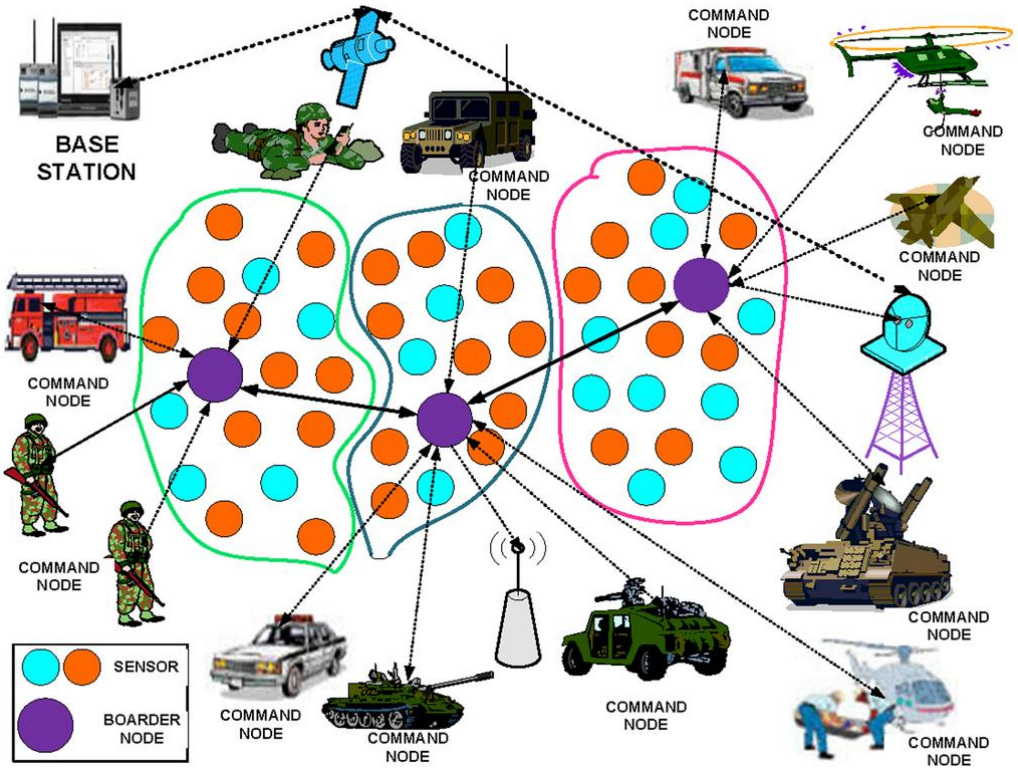
کاهش مصرف انرژی در لایه فیزیکی نیازمند عملیات کم مصرف است. مصرف انرژی در لایه فیزیکی به خاطر انرژی مورد نیاز مدارات و ارتباطات است. ارسال کننده و دریافت کننده برای فعال نمودن مداراتشان نیاز به انرژی دارند. برای شروع یک فرستنده، میزان قابل توجهی زمان و انرژی لازم است. در برخی موارد انرژی راه اندازی بیش از انرژی مورد نیاز برای ارسال واقعی است. برای فرستنده ای که میان حالات خواب و بیداری سوئیچ می کند، معماری راه اندازی فرستنده سریعی برای کمینه کردن انرژی و زمان مورد نیاز است.

طرح مدولاسیون مورد استفاده یک رادیو می تواند روی انرژی مصرفی گره تاثیر بگذارد. بنابراین طرح های مدولاسیون کارا–از لحاظ انرژی برای کاهش انرژی مصرفی مورد نیاز است.

خوشه بندی در شبکه حسگر بی سیم

در بین پروتکل های خوشه بندی ارائه شده برای شبکه حسگر بی‌سیم، پروتکل خوشه بندی LEACH اهمیت ویژه ای بین محققین این حوزه پیدا کرده است. از دلایل اهمیت پیدا کردن این پروتکل خوشه بندی، می توان به ویژگی های خاصی تشکیل خوشه در این پروتکل اشاره نمود که عبارتند از:

- *تصادفی*
- *تطبیقی*
- *خودپیکربندی*



خوشه بندی تصادفی

به این معنی که در هر دور(Round) ، تعداد مشخصی از گره ها به صورت تصادفی خود را به عنوان سرخوشه انتخاب می کنند. نقش سرپرستی خوشه، از قبل برای گره های خاصی در نظر گرفته نمی شود.

خوشه بندی تطبیقی

گره هایی که در دور فعلی نقش سرخوشه را به عهده داشته اند، در دور بعدی دیگر نمی توانند برای بر عهده گرفتن این نقش، کاندید شوند. بنابراین انتخاب کاندیدهای سرپرستی خوشه در هر دور، با توجه به دور قبلی مشخص می شود. بدین ترتیب، انتظار می رود که پس از سپری شدن چند دور مشخص، تمامی گره ها حداقل یک مرتبه، به عنوان سرخوشه، انتخاب شده باشند. البته بعداً خواهیم دید که لزوماً این اتفاق نمی افتد.

خوشه بندی خودپیکربندی

گره های شبکه در این پروتکل خوشه بندی بدون کمک هر عامل خارجی و یا گره‌ی خاصی از شبکه، تشکیل خوشه می دهند. این موضوع به مقیاس پذیری پروتکل خوشه بندی لیچ (Leach) کمک می کند. همان‌طور که در ادامه خواهیم دید، تغییرات زیادی برای بهبود کارآیی پروتکل خوشه بندی leachتوسط محققین انجام شده است. ولی متأسفانه در اکثر آن‌ها این ویژگی از بین رفته است و یک گره خاصی وظیفه ی انتخاب سرخوشه ها را بر عهده می گیرد. این مسئله تأثیر منفی روی مقیاس پذیری شبکه می گذارد.

در پروتکل خوشه بندی **LEACH** یک سری قوانین کلی وجود دارد که برای آشنایی بیشتر با این پروتکل، به مرور این قوانین می پردازیم:

۱ -در هر دور، تعداد مشخصی از گره ها به صورت تصادفی خود را به عنوان سرخوشه انتخاب می کنند. نقش سرخوشه بودن، از قبل برای گره های خاصی در نظر گرفته نمی شود.

۲ -گره هایی که در دور فعلی نقش سرخوشه را به عهده داشته اند، در دور بعدی دیگر نمی توانند برای بر عهده گرفتن این نقش، کاندید شوند. بنابراین انتخاب کاندیدهای سرخوشه در هر دور، با توجه به دور قبلی مشخص می شود. بدین ترتیب، انتظار می رود که پس از سپری شدن چند دور مشخص، تمامی گره ها حداقل یک مرتبه، به عنوان سرخوشه ، انتخاب شده باشند .البته بعداً خواهیم دید که لزوماً این اتفاق نمی افتد.

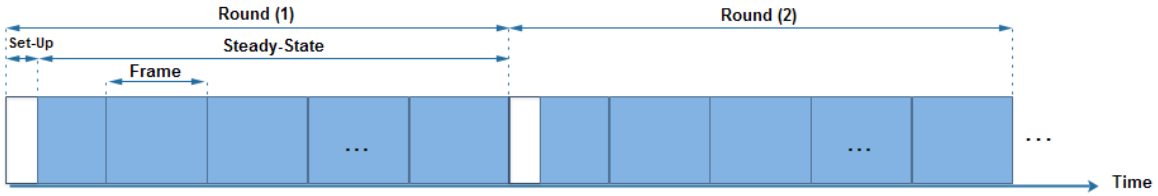
۳ -گره های شبکه در این پروتکل بدون کمک هر عامل خارجی و یا گره ی خاصی از شبکه، تشکیل خوشه می دهند. این موضوع به مقیاس پذیری این پروتکل کمک می کند. همان‌طور که در ادامه خواهیم دید، تغییرات زیادی برای بهبود کارایی این پروتکل توسط محققین انجام شده است. ولی متأسفانه در اکثر آن‌ها این ویژگی از بین رفته است و یک گره خاصی وظیفه ی انتخاب سرخوشه را بر عهده می گیرد. این مسئله تأثیر منفی روی مقیاس پذیری شبکه می گذارد.۴– انتقال اطلاعات از گره های یک خوشه به سرخوشه و از سرخوشه ها به ایستگاه پایه با کنترل محلی انجام می شود و نیازی به کمک یک عامل خارجی و یا گره‌ی خاصی در شبکه برای انتقال اطلاعات نیست.

۵ -پروتکل MAC استفاده شده در LEACH با فراهم آوردن ویژگی Sleep برای مصرف انرژی، به مقدار مناسبی در مصرف انرژی گره ها صرفه جویی می کند.

۶ -پکت هایی که در پروتکل LEACH بین گره های حسگر رد و بدل می شود، دارای یک فیلد برای تعیین نوع پکت هستند که برای تصمیم گیری در مورد نحوه برخورد با پکت های مختلف از این فیلد استفاده می شود.

۷ -در پروتکل LEACHزمان به قسمت هایی با طول مساوی به نام دور (Round)تقسیم می‌شود. هر دور نیز از لحاظ اجرایی، به دو فاز تقسیم می شود:

-
  - فاز۱– راه اندازی**(Set-up)**
  - فاز۲– حالت پایدار**(Steady-State)**



فاز راه اندازی نیز خود به دو مرحله تقسیم می شود.

- مرحله انتخاب سرخوشه
- مرحله تشکیل خوشه

۸ -در مرحله انتخاب سرخوشه، گره ها به صورت تصادفی و بر اساس یک تابع احتمال، سرخوشه می شوند.

۹ -در مرحله تشکیل خوشه نیز گره ها درخواست عضویت خود را به سرخوشه ها ارسال می کنند تا سرخوشه ها بر اساس یک سری معیارها، اعضای خود را انتخاب کنند.

پلفترم اینترنت اشیا IoT Platform

پلتفرم مجموعه‌ای از خدمات مورد نیاز برای پیاده سازی اینترنت اشیا می‌باشد. بازار پلتفرم‌ها در حال حاضر مشابه بازار موتورهای جستجو در دهه ۹۰ میلادی است. رقابت زیاد و بازار نوپا یکی از دلایل این تشبیه است. بنابراین با توجه به امکانات امروزی، بی دلیل نیست اگر هر روز و هر ماه شاهد پلتفرم‌های جدید باشیم. به صورت کلی **پلتفرم اینترنت اشیا IoT Platform** نقش بسیار مهمی در معماری اینترنت اشیا دارد. یک سناریو اجرا شده از اینترنت اشیا را در نظر بگیرید، دستگاه‌های متصل شده به همدیگر، اطلاعاتشان را روی **پلتفرم** بر بستری ابری ارسال می‌کنند. پلتفرم IoT اطلاعات را (معمولا در فضای ابری) ذخیره کرده و از آن‌ها جهت ایجاد نمودار استفاده می‌کند. به عبارت دیگر، یک سرویس ابری اینترنت اشیا مانند PaaS عمل می‌کنند. اگر معنی این عبارت را نمی‌دانید، در بخش نظرات همین پست سوال بپرسید. این PaaS سرویس‌های کاربردی مهمی را ارایه می‌دهد. از جمله امکان ارتباط سخت افزارها به یک سرویس ابری مشترک جهت تحلیل و بررسی اطلاعات می‌باشد.

در مبحث اینترنت اشیا با تکنولوی‌ها و سخت افزارهای مختلفی در ارتباط هستیم. قبل از اینکه راجع به انتخاب پلتفرم توضیح بدهم، لازم است بدانیم که **پلتفرم** چیست. سناریو را به این صورت در نظر می‌گیریم. سنسورها از طریق یک برد امبدد مانند آردوینو یا ESP۸۲۶۶ اطلاعات را از محیط دریافت می‌کنند. این اطلاعات به تنهایی کاربردی ندارند. در ابتدای امر بایستی به سرور منتقل شوند. پس از آن در سرور ذخیره شوند، سپس اقدامات تحلیل و visualizationروی آن‌ها صورت گیرد. عملیات دسته بندی و دریافت اطلاعات از سنسورها و سخت افزارها توسط پلتفرم صورت می‌گیرد. چند پلتفرم کاربردی در حوزه اینترنت اشیا را معرفی خواهم کرد .

نیازهای پلتفرم IoT Platform

به صورت عمومی یک **پلتفرم اینترنت اشیا** باید حداقل امکانات زیر را ارایه بدهد.

- دریافت اطلاعات
- تبدیل و انتقال اطلاعات
- امکان ساخت داشبوردهای مختلف
- امکان تعریف قوانین پایه در معماری IoT
- مدیریت سخت افزارها از جمله انواع بردها
- تضمین امنیت در تبادل و ذخیره اطلاعات دریافتی
- سازگاری با انواع پلتفرم‌ها جهت تبادل و دریافت اطلاعات

پلتفرم Google IoT Cloud

این پلتفرم یکی از جذاب‌ترین و پرکاربردترین **پلتفرم IoT** می‌باشد. گوگل یکی از بزرگترین شرکت‌ها در دنیای دیجیتال می‌باشد. بدون شک تمامی سرویس‌های گوگل کاربردی بوده و سرعت به روزرسانی بسیار زیادی دارند. ابزارهای گسترده زیادی در این پلتفرم برای مدیریت سمت سخت افزار و سمت سرور ارایه می‌شوند. دستگاه‌های متصل شده به این پلتفرم از سرویس Pub/Sub جهت انتشار اطلاعات می‌توانند استفاده کنند. نقطه قوت در **پلتفرم Google IoT Cloud** امکان استفاده از دیگر سرویس‌ها قدرتمند گوگل در این پلتفرم می‌باشد. از جمله سرویس BigQuery که منحصرا برای تحلیل دیتاهای حجیم طراحی شده است. حتی امکان افزودن یادگیری ماشینی به این اطلاعات هم وجود دارد. همانند دیگر سرویس‌های گوگل هم این سرویس دارای مخازن اطلاعاتی کاربردی از جمله فیلم و متن می‌باشد. دلایل زیادی برای استفاده از یک سرویس کامل و حرفه‌ای وجود دارند. ولی متاسفانه این سرویس کاربردی هم همانند سرویس‌های کاربردی دیگری از جمله Google Business هم در ایران کارایی نخواهند داشت.

پلتفرم AWS IoT Core

پلتفرم اینترنت اشیا بربستر سرویس ابری آمازون می‌باشد. سرویس AWS یک سرویس ابری بسیار کاربردی از سمت آمازون می‌باشد. هسته پلتفرم اینترنت اشیا آمازون به این بستر پایبند می‌باشد. مهم‌ترین نقطه قوت این **پلتفرم اینترنت اشیا IoT Platform** تضمین امنیت پروژه‌های IoT میباشد. علت آن هم مشخص است، سرویس ابری AWS کاملا براین حوزه تسلط دارد. امکان دریافت اطلاعات از انواع سخت افزارهای متصل شده به این سرویس و اعمال فعالیت‌های Real-time روی آن‌ها، یکی دیگر از نقاط قوت این سرویس می‌باشد. سرویس‌های ارایه شده از پلتفرم **AWS IoT Core** به شرح زیر می‌باشد.

- پشتیبانی از RTOS که یک سیستم عامل برای بردهای امبدد می‌باشد.
- پشتیبانی از AWS Greengrass که یک نرم افزار سبک جهت اجرای فرآیندهای محاسباتی سمت سخت افزار میباشد.
- پشتیبانی از AWS IoT Analytics که یک سرویس پیشرفته تحلیل دیتا می‌باشد.

- پشتیبانی از AWS IoT device management که یک سرویس کاربردی جهت ساده سازی ارتباط و مدیریت سخت افزارها میباشد. مخصوصا وقتی تعداد دستگاه‌ها زیاد باشد.
- پشتیبانی از AWS IoT Core به عبارتی هسته اصلی این پلتفرم می‌باشد. امکان برقراری ارتباط با پلتفرم ابری را فراهم می‌کند.

پلتفرم Artik Cloud

پلتفرم اینترنت اشیا Artik Cloud توسط سامسونگ ایجاد شده است. نکته جالب در خصوص روال کار این پلتفرم، امکان ارتباط بین سخت افزارها و ارتباط آن‌ها با سرویس ابری می‌باشد. نقطه قوت آن هم در سرعت تنظیم کردن و تبادل اطلاعات بین سخت افزارهای مختلف و پلتفرم ابری می‌باشد. همچین دارای بخشی جهت ایجاد ارتباط با پلتفرم‌های دیگر را دارد. همانطور که در دوره اسپارکرینار هم توضیح دادم، یکی از نکاتی که باعث پیشرفت پلتفرم‌ها می‌شود. امکان سازگار سازی با یکدیگر می‌باشد. به این چند روش امکان دریافت اطلاعات از سنسورهای مختلف و تجمیع سازی آن‌ها در پلتفرم اینترنت اشیا سامسونگ Artik Cloud فراهم می‌شود. در آخر هم این پلتفرم با ارایه SDK امکان ساده سازی فرایند توسعه را در اختیار کاربران قرار می‌دهد.

پلتفرم Microsoft Azure IoT

پیرو ادعای مایکروسافت این پلتفرم یکی از قوی‌ترین پلتفرم‌های اینترنت اشیا می‌باشد. نمی‌دانم چرا، ولی مایکروسافت اعلام کرده که این پلتفرم امکان برقراری ارتباط دو طرفه بین سخت افزارها و پلتفرم Azure وجود دارد! کار بسیار مهم پلتفرم همین موضوع می‌باشد. البته اعلام کرده که این فرایند با پروتکل‌های استاندارد صورت می‌گیرد! ولی نکته مثبت این پلتفرم پشتیبانی از تصدیق سخت افزاری است. این مورد به امنیت پلتفرم **Microsoft Azure IoT** مایکروسافت کمک می‌کند. مانند دیگر پلتفرم‌های اینترنت اشیا، Azure هم فرایندها را ساده می‌کند.

جمع بندی پلتفرم اینترنت اشیا IoT

در کل از هر گوشه و کناری پلتفرم اینترنت اشیا متولد شده است. هر کدام با ویژگی‌های خاص و البته تمرکز بر بخشی از بازار در حال جمع آوری کاربر و اطلاعات هستند. از آنجایی که این بازار با سرعت بسیار زیادی در حال رشد می‌باشد. همچنین گردش مالی بسیاری هم در این حوزه وجود دارد که روز به روز بیشتر هم خواهد شد. طبیعتا پلتفرم‌های مختلف زیر نظر سازمان و شرکت‌ها خاص در حال ارایه خدمات جهت جمع آوری اطلاعات و جمع آوری کاربران می‌باشند. سرمایه گذاری‌های زیادی در این حوزه روی استارتاپ‌ها صورت گرفته و بازهم در حال رشد می‌باشد. کلام آخر اینکه جهش در این حوزه فقط با ایجاد پلتفرم صورت نمی‌گیرد. جهش در حوزه IoT با حضور اسپارکرها صورت خواهد گرفت.

ده سوالی که باید قبل از انتخاب یک پلت فرم، از خودتان بپرسید

#	محدوده عملیاتی پلت فرم	سوال	پاسخ اهمیت دارد وقتیکه :
1	نرم افزارها	آیا پلت فرم امکان توسعه، آزمایش و نگهداری چندین نرم افزار را فراهم میکند؟	شما قصد دارید تعداد قابل توجهی نرم افزار اختصاصی را خودتان توسعه دهید.
2		آیا پلت فرم قابلیت ترجمه زبانهای موجود نرم افزارها را دارد؟	امکانات توسعه شما ابتدایی است یا اینکه شما به دنبال راهکاری اماده برای مشکل کسب و کار خود هستید.
3		آیا پلت فرم به راحتی به نرم افزارهای فعلی کسب و کار شما متصل میشود؟ (مثل ERP,MES)	لازم است بیشترین ارزش افزوده از داده های حاصل از برنامه های IOT حاصل شود.
4	مدیریت داده ها	آیا پلت فرم امکان ساختارسازی و برقراری ارتباط بین چندین بسته داده غیر مرتبط را دارد؟	شما منابع متعددی از داده ها دارید که ساختار ندارند، متمرکز نیستند، یا از 3rd Party می آیند.
5		آیا پلت فرم میتواند جریان داده های با سرعت بالا را سریع دریافت کند؟	حجم داده ها زیاد است، به خصوص در لبه، یا اینکه آنالیزور ها نیاز به تصمیم گیری و کنترل داده ها در لحظه را دارند.
6		پلت فرم چگونه عملیات پاکسازی، فرمت کردن، و اصلاح داده ها را مدیریت میکند؟	منابع داده مستعد به خطا هستند، به خوبی قابل فهم یا قابل کنترل نیستند.
7	زیرساخت	آیا ارائه دهنده پلت فرم، مرکز داده و فضای ابری اختصاصی خود را دارد؟ در غیر این صورت از کدام تامین کننده فضای ابری عمومی استفاده میکند؟	نیاز به یک فضای ابری اختصاصی دارید، یا مشخصه های خاص جغرافیایی برای ذخیره سازی داده ها دارید، یا اینکه اصلا نیاز ندارید که پلت فرم شما روی فضای ابری اختصاصی اداره شود و یا در مکان کسب و کار شما استقرار یابد.
8	امنیت	پلت فرم چه قابلیتهای احراز هویت، کد گذاری و نظارت را در حد کسب و کارها دارد؟ آیا بخشی از این قابلیتها متمایز هستند؟	شما میخواهید/ نیاز دارید که یک استاندارد ویژه برای امنیت و حریم خصوصی داشته باشید، یا اینکه از داده ها برای اخذ تصمیمات مالی و عملیاتی فوری استفاده میکنید.
9	فرآیندهای لبه	آیا پلت فرم توانایی تحلیل داده ها را در لبه دارد بدون اینکه در ابتدا اطلاعات به فضای ابری انتقال یابد؟	پهنای باد و ارتباط محلی یا داخلی گران است، و یا وقتی که نیاز است تصمیمات داخلی به سرعت اتخاذ شود.
10		آیا پلت فرم به راحتی قابل برنامه ریزی برای کنترل دارایی های محلی بدون دخالت انسان میباشد؟	شما نیاز دارید که دستگاه هایتان در لبه امکان تنظیم یا تغییر وضعیت را بدون دخالت انسان، داشته باشند.

حفظ حریم خصوصی در اینترنت اشیا(IoT)

همان طور که در قبلا بیان شد، شبکه اینترنت اشیا شامل دستگاه های مختلفی است که با یکدیگر در حال تعامل هستند. این دستگاه ها برای انجام بسیاری از امور نیاز به اطلاعات کاربر داشته یا در حال نگهداری داده های بسیاری هستند که حفظ و امنیت آن ها برای مصرف کننده بسیار حائز اهمیت است. در بین تمام چالش های امنیتی که اینترنت اشیا با آن روبه رو است، حفظ حریم خصوصی جایگاه ویژه ای دارد. زیرا عدم اطمینان کاربر به چگونگی حفظ حریم خصوصی و نگرانی در رابطه با افشای اطلاعات سبب می شود تمایلی به استفاده از IoT نداشته باشد. از جمله مهم ترین نیازمندی های حفظ حریم خصوصی در اینترنت اشیا عبارتست از:

۱- ایجاد پروتکل های امنیتی با قابلیت مخفی کردن اطلاعات شخصی و خصوصی
۲- عدم امکان ردیابی دستگاه ها توسط دستگاه های غیرمرتبط دیگر
۳- تنظیم پروتکل هایی به منظور جلوگیری از نشت اطلاعات و حفظ حریم شخصی
۴- تنظیم قوانین به صورت مکتوب و واضح به منظور اطلاع رسانی کاربر در حین صدور مجوز
۵- حفظ حریم خصوصی هنگام استفاده از دستگاه ها
۶- حفظ حریم خصوصی با امکان استفاده از شرایط گمنامی برای دستگاه هایی که نیاز به اطلاعات هویتی ندارند
۷- امکان حذف و پاک کردن کامل اطلاعات پس از استفاده کاربر به منظور جلوگیری از سواستفاده های احتمالی آینده

چالش های امنیتی اینترنت اشیا(IoT)

در اینترنت اشیا از دستگاه های مختلفی استفاده می شود که ممکن است با تکنولوژی های ارتباطی متفاوتی با یکدیگر در حال تعامل باشند. همین امر چالش های مختلفی را از نظر امنیتی به دنبال خواهد داشت. برخی از مهم ترین چالش ها عبارتند از:

نیاز به امن سازی دستگاه های متفاوت به دلیل استفاده از فناوری ها و دستگاه های متعدد که هر کدام آسیب پذیری های خاص خود را دارند

عدم امکان استفاده از مکانیزم های دفاعی متمرکز به دلیل قابلیت مقیاس پذیری و گسترده بودن دستگاه های IoT

متفاوت بودن نیازمندی های امنیتی دستگاه های مختلف به دلیل کاربرد متفاوت هرکدام در سطح کاربر، دولت و سازمان ها

افزایش میزان داده ها و اطلاعات و نیاز به مکانیزم امنیتی قوی برای جلوگیری از وقوع مشکل برای داده ها

نیاز به حفاظت در برابر حملاتی که سرویس دهی را دچار اختلال زمانی می کنند برای دستگاه هایی که به سرویس دهی حداقل تاخیر نیاز دارند

پیش بینی حملات سایبری به منظور جلوگیری از انجام یا وقوع آن ها روی دستگاه ها یا شبکه اینترنت اشیا

انواع حملات در اینترنت اشیا(IoT)

شبکه اینترنت اشیا از مولفه های مختلفی همچون دستگاه ها و انسان و پروتکل های ارتباطی تشکیل شده است. این مولفه ها باید با کمک فرآیندهای امنیتی در مقابل حملات مختلف مقاوم باشند. به منظور آمادگی بیشتر برای مقابله و پیش بینی حملات مختلف، نیاز است با حملات مختلف در این زمینه آشنا شد. در ادامه به مهم ترین حملات ممکن در شبکه اینترنت اشیا خواهیم پرداخت.

۱- حمله مبتنی بر میزبان یا Host Based Attack

در شبکه اینترنت اشیا، میزبان های مختلفی ممکن است وجود داشته باشند که هر کدام سطح امنیتی مخصوص به خود را دارند. وجود میزبان های مختلف که می توانند سخت افزار یا نرم افزارهای متفاوت باشند، امکان حمله مبتنی بر میزبان را افزایش می دهد. در این گونه از حملات، مهاجم آسیب پذیری های سخت افزار یا نرم افزار را شناسایی کرده و حمله خود را متناسب با آن انجام می دهد.

۲- حمله جعل یا Spoofing Attack

همان طور که در مقاله اسپوفینگ (Spoofing) چیست؟ بیان شد، این حمله به معنای جعل کردن یک یا چند المان از یک ارتباط است به طوریکه کاملا قابل اعتماد و مشخص به نظر برسد. این حمله می تواند زمینه ساز بسیاری از حملات دیگر همچون حمله تکرار، حمله منع سرویس و ... در IoT شود. در این حمله معمولا نقاط ورود اطلاعات بیشتر مورد توجه مهاجم قرار می گیرد.

۳- حمله منع سرویس یاDoS Attack

این حمله یکی از رایج ترین حملات در اینترنت اشیا است که سبب منع دسترسی به دستگاه ها و برآورده کردن نیاز کاربران خواهدشد. در واقع کاربران با انجام این حمله به منابع و سرورها دسترسی نخواهند داشت. اگر این حمله به صورت توزیع شده انجام شود به آن منع سرویس توزیع شده یا DDoS Attackمی گویند که در مقاله حمله DDoS یا دیداس چیست؟ به طور کامل به آن پرداخته شده است.

۴- حمله Sybil

در این حمله مهاجم می تواند در یک زمان چند هویت داشته و امنیت و یکپارچگی داده ها را در شبکه اینترنت اشیا تهدید کند. در واقع مهاجم در عین داشتن هویت های متعدد سعی بر عادی نشان دادن موقعیت خود خواهدداشت. در این حمله، مهاجم سعی می کند رفتار عادی از خود نشان دهد و امنیت دستگاه ها را به خظر اندازد.

۵- حمله مبتنی بر ویژگی دستگاه ها

در این حمله، مهاجم ویژگی های هر دستگاه در اینترنت اشیا مورد توجه قرار داده و با توجه به آن سعی می کند به گونه ای در پردازش یا توان محاسباتی و ...دستگاه اختلال ایجاد کند یا با دادن اطلاعات و داده های اشتباه سبب گمراهی در کارکرد آن ها شود. ساختار این حملات بنا به خصوصیات دستگاه ها می تواند متفاوت باشد.

۶- حمله وقفه یاInterruption Attack

در این حملات مهاجم سعی دارد دستگاه ها را از دسترس خارج کنند و شبکه IoTرا دچار اختلال کنند. برای این کار مهاجم ممکن است راه های مختلفی را امتحان کند. به بیان بهتر هر روشی که سبب اختلال در کار دستگاه یا شبکه شود یا آن را از کار بیندازد، می تواند یک حمله وقفه باشد.

۷- حمله مرد میانی یاMan-in-the-Middle Attack

در این حمله، همان طور که در مقاله حمله مرد میانی یا Man in the Middle چیست؟ بیان شد، مهاجم بین دستگاه های مختلف یا بین دستگاه و کاربر در شبکه IoT قرار گرفته و اطلاعاتی که در حال رد و بدل شدن هستند را با توجه به اهداف خود تغییر می دهند. برای این کار مهاجم باید بین دستگاه ها یا کاربر و دستگاه هایی که در حال تعامل و ارتباط هستند قرار گرفته و ارتباط را شنود می کند و به گونه ای رفتار می کند که کسی از خارج متوجه غیرقانونی بودن حضور او در این تعامل نشود.

۸- حمله Fabrication

در این حمله مهاجم اقدام به جعل هویت شخص دیگری کرده و داده ها و اطلاعات نادرست را به عنوان آن شخص به اشتراک می گذارد. در واقع مهاجم اقدام به تولید پیام های ساختگی می کند و آن را به شخص دیگری نسبت می دهد .این کار سبب آشفتگی در شبکه IoT خواهد شد.

حمله سطح دسترسی یاAccess Level Attack

هر دستگاه و هر کاربر در اینترنت اشیا سطح دسترسی مشخصی دارد. با این حمله ممکن است سطح دسترسی غیرمجاز پیدا کنند و به شیوه ای نامتعارف، اطلاعات حساس را به دست آورند. همچنین این حملات ممکن است مکانیزم های دسترسی اشتراکی به منابع را دچار اختلال کنند.

۹- حمله به پایگاه دادهIoT

حملات SQL Injection یا حملات دیگر همچون XSS به پایگاه داده اینترنت اشیا از جمله رایج ترین حملاتی هستند که توسط مهاجمان علیه دستگاه های IoT در حال انجام است. در واقع احراز هویت ضعیف یکی از عواملی است که می تواند سبب نفوذ به دستگاه ها و به خظر انداختن اطلاعات آن ها شود. در مقاله انواع آسیب پذیری های برنامه های تحت وب به طور کامل در رابطه با چگونگی این حملات توضیح دادیم.

۱۰-حمله مبتنی بر پروتکل یاProtocol Based Attack

در این حمله مهاجم سعی در ایجاد اختلال در برخی از پروتکل های امنیتی به خصوص پروتکل های مربوط به حریم خصوصی در IoT دارد تا با کمک آن برخی از پروتکل های امنیتی را نقض کرده و عملیات مورد نظر خود را انجام دهد. برخی از این حملات با هدف شکستن پروتکل های رمزنگاری که برای انتقال داده ایمن بین دستگاه های اینترنت اشیا با یکدیگر یا با کاربر استفاده می شود، انجام می شوند.

دستگاه های اینترنت اشیا روز به روز در حال گسترش و متنوع شدن هستند. به همین دلیل گستردگی حملات تنها به موارد ذکرشده محدود نمی شود. این حملات برخی از مهم ترین و اصلی ترین حملاتی بودند که ممکن است اینترنت اشیا با آن مواجه شود.

راهکارهای افزایش امنیت اینترنت اشیا(IoT)

اگرچه چالش ها و تهدیدات امنیتی بسیاری برای اینترنت اشیا وجوددارد اما با ارائه و پیاده سازی راهکارهایی می توان آن ها را تا حد خوبی کاهش داد . برخی از این راهکارها عبارتند از:

۱- استفاده از سیستم تجزیه و تحلیل و نظارت امنیتی به منظور نگهداری و شناسایی الگوهای استفاده شده و مقایسه آن با الگوهای جدید و تشخیص خرابکاری احتمالی و نشان دادن عکس العمل نسبت به آن

۲- استفاده از سیستم احراز هویت دو طرفه به منظور اطمینان از اعتبار دستگاه هایی که به شبکه اینترنت اشیا متصل می شوند پیش از انتقال یا دریافت داده

۳- استفاده از بوت امنیتی یا Secur boot که یک استاندارد امنیتی است و به منظور اطمینان از بوت شدن دستگاه با استفاده از نرم‌افزاری که مورد اعتماد سازنده تجهیزات اصلی (OEM) است، تهیه‌شده و سبب جلوگیری از حمله مرد میانی خواهدشد.

استاندارد جهانی امنیت اینترنت اشیا یاIoT

به دنبال فراگیرشدن استفاده از دستگاه های اینترنت اشیا و نگرانی از چالش های امنیتی آن ها، موسسه استاندارد ارتباطات اروپا(ETSI) ، اولین نسخه از استاندارد جهانی برای امنیت سایبری در اینترنت اشیا با مشخصه TS ۱۰۳۶۴۵ را با هدف معرفی استانداردی پایه برای صدور گواهینامه های دستگاه هایIoT ، ارائه داد. این نسخه الزامات امنیتی را برای اجراکنندگان و ارائه دهندگان اینترنت اشیا ایجاد می کند. برای مثال طبق این استاندارد، در دستگاه های IoTامکان استفاده از رمزهای عبور پیش فرض که در جهان متداول است و سبب بسیاری از مسائل امنیتی خواهدشد، وجود نداشته باشد. همچنین باید ابزارهایی به منظور مدیریت گزارش های آسیب پذیری سیستم ها در نظر گرفته شود. این نسخه امنیتی همچنین ارائه دهندگان را ملزم به، به روزرسانی نرم افزارها و تضمین یکپارچگی آن ها به منظور اطمینان از حفظ اطلاعات شخصی و جلوگیری از حمله مهاجمان می کند. استاندارد معرفی شده، مقررات دیگری از جمله آسان کردن فرایند حذف اطلاعات شخصی توسط کاربران، نگهداری آسان و مناسب دستگاه ها، بررسی داده های تله متری و اعتبار دستگاه ها را نیز شامل می شود.

سخن پایانی

اینترنت اشیا اگرچه سبب تسهیل در انجام بسیاری از امور می شود اما چالش های امنیتی بسیاری به دلیل استفاده از پروتکل ها و دستگاه های مختلف می تواند به دنبال داشته باشد. به همین منظور شناسایی نقاط ضعف دستگاه ها و پروتکل ها و آشنایی با خطراتی که می تواند IoT را تهدید کند، می تواند در کاهش این چالش ها کمک کننده باشد. به همین منظور در این مقاله به چالش های امنیتی و خطراتی و حملاتی که IoT را تهدید می کند و هچنین راه های کاهش این خطرات پرداختیم.