وزارت ارتباطات و فناوری اطلاعات
پژوهشگاه ارتباطات و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)
ITRC

**پژوهشکده امنیت ارتباطات و فناوری اطلاعات**
گروه فناوری امنیت اطلاعات و سامانه‌ها

# نام گزارش:

## شناسایی مراکز تحقیقاتی، چالش‌ها و راه‌حل‌ها در امنیت اینترنت اشیا

**مستخرج از پروژه:**

**تحلیل چالش‌های امنیتی در اینترنت اشیاء**

**کد پروژه: ۹۳۳۵۲۱۳**

مجری: محمد حسام تدین

به نام خدا


**پژوهشکده امنیت ارتباطات و فناوری اطلاعات**

# نام گزارش: شناسایی مراکز تحقیقاتی، چالش‌ها و راه‌حل‌ها در امنیت اینترنت اشیا

**پروژه: تحلیل چالش‌های امنیتی در اینترنت اشیاء**

**کد پروژه: ۹۳۳۵۲۱۳**

| | |
|---|---|
| **مجری:** | **محمد حسام تدین** |
| **تهیه‌کننده:** | **محمد حسام تدین، نسرین تاج، عاطفه ترکمن** |
| **کد گزارش:** | IOT_Sec phase 1 |
| **تاریخ ارائه:** | **۹۴/۱/۳۰** |
| **نسخه/وضعیت:** | **نهایی** |


خواننده گرامی، در راستای تحقق ماموریت پژوهشگاه ارتباطات و فناوری در فراهم سازی سکویی برای ارتقاء دانش، انتقال فناوری و بومی‌سازی محصولات و خدمات حوزه فاوا و با هدف جلب مشارکت علاقه‌مندان در توسعه و بهره مندی از دستاوردهای پژوهشگاه ارتباطات و فناوری اطلاعات، آزاد رسانی این دستاوردها در زمره برنامه های اولویت دار پژوهشگاه به شمار می‌آید. به همین منظور مستند حاضر تحت مجوز بین المللی **CC-BY-SA-NC** نسخه ۴، در دسترس عموم قرار گرفته است.

شایان ذکراست تحت این مجوز، ضمن حفظ کلیه حقوق مالکیت فکری این مستند برای پژوهشگاه ارتباطات و فناوری اطلاعات، بازانتشار و بکارگیری آن صرفاً برای موارد تحقیقاتی و با ذکر نام **پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)** بلامانع است.

# شناسنامه گزارش

| | | |
|---|---|---|
| **عنوان: شناسایی مراکز تحقیقاتی، چالش‌ها و راه‌حل‌ها در امنیت اینترنت اشیا** | | **شماره نسخه: ۱** |
| **کد:** IOT_Sec phase 1 | **نوع گزارش: مطالعاتی** | **تاریخ ارائه گزارش:** ۹۴/۱/۳۰ |
| **نام پروژه: تحلیل چالش‌های امنیتی در اینترنت اشیاء** | | **نوع پروژه: راهبردی** |
| **تاریخ شروع: ۹۳/۱۱/۱۹** | | **تاریخ پایان: ۹۴/۴/۱۹** |
| **نام گروه: فناوری امنیت اطلاعات و سامانه‌ها** | | |
| **مجری: محمد حسام تدین** | | **ناظر / ناظرین: مهندس سید هادی سجادی** |
| **تهیه کننده/ تهیه کنندگان: محمد حسام تدین، نسرین تاج، عاطفه ترکمن** | | |
| **نام و نشانی مجری: محمد حسام تدین، پژوهشکده امنیت ارتباطات و فناوری اطلاعاز** | | |
| **نام و نشانی حمایت کننده:**<br>تهران، انتهای خیابان کارگر شمالی، پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)_کد پستی: ۱۴۳۹۹۵۵۴۷۱_ تلفن: ۱۰-۸۰۰۵۵۰۸ | | |
| **ملاحظات:** - | | |
| **چکیده:**<br>اینترنت اشیاء، یک فناوری نوظهور است که به سمت فراگیر شدن پیش می‌رود و زندگی انسان‌ها را تحت الشعاع خود قرار خواهد داد. در این گزارش، پس از معرفی اینترنت اشیاء و مزیت‌ها و کاربردهای آن، امنیت در اینترنت اشیاء به عنوان یک محور کلیدی مورد توجه قرار می‌گیرد و نیازمندی‌ها، چالش‌ها و راه‌حل‌های پیشنهادی برای آن مطرح می‌شود. همچنین مراکز تحقیقاتی و پژوهشی فعال در این حوزه و پروژه‌های تحقیقاتی مورد توجه آنها بررسی می‌گردد. | | |
| **کلمات کلیدی:**<br>**اینترنت اشیاء، نیازمندی‌ها و چالش‌های امنیتی، حریم خصوصی و اعتماد، معماری امنیتی** | | |
| **وضعیت گزارش: نهایی** | | **زبان گزارش: فارسی** |
| **وضعیت دسترسی: عادی** | | **تعداد صفحات: ۲۱۲** |

## چکیده

اینترنت اشیاء، یک فناوری نوظهور است که به سمت فراگیر شدن پیش می‌رود و زندگی انسان‌ها را تحت الشعاع خود قرار خواهد داد. در این گزارش، پس از معرفی اینترنت اشیاء و مزیت‌ها و کاربردهای آن، امنیت در اینترنت اشیاء به عنوان یک محور کلیدی مورد توجه قرار می‌گیرد و نیازمندی‌ها، چالش‌ها و راه‌حل‌های پیشنهادی برای آن مطرح می‌شود. . همچنین مراکز تحقیقاتی و پژوهشی فعال در این حوزه و پروژه‌های تحقیقاتی مورد توجه آنها بررسی می‌گردد. مراجع استفاده شده برای این گزارش، در ابتدای هر بخش ارائه شده است و در کنار موضوعات مربوطه قرار دارد.

# تقدیر و تشکر

از آقایان مهندس هادی خان محمدی، سیاوش احمدی و اشکان دیوبند به خاطر کمک‌های ایشان در انجام پروژه تقدیر و تشکر می‌گردد. همچنین از ناظر محترم، جناب آقای مهندس سید هادی سجادی به خاطر نظرات ارزشمندشان تشکر می گردد.

# سرفصل مطالب

# فهرست جداول

# فهرست اشکال

## ۱- مقدمه

در این فاز سعی شده است به طور وسیعی مراکز پژوهشی معتبر، شرکت‌های فعال، دانشگاه‌های مطرح که در زمینه اینترنت اشیا و خصوصا امنیت اینترنت اشیا به طور جدی و فعال مشغول کار هستند شناسایی شوند، تا مبتنی بر فعالیت های صورت گرفته ایشان بتوان در فاز دوم پروژه با یک نتیجه‌گیری اصولی برای تهیه یک برنامه پژوهشی اقدام نمود. اینترنت اشیاء، یک فناوری نوظهور است که به سمت فراگیر شدن پیش می‌رود و زندگی انسان‌ها را تحت الشعاع خود قرار خواهد داد. در این گزارش، پس از معرفی اینترنت اشیاء و مزیت‌ها و کاربردهای آن، امنیت در اینترنت اشیاء به عنوان یک محور کلیدی مورد توجه قرار می‌گیرد و نیازمندی‌ها، چالش‌ها و راه‌حل‌های پیشنهادی برای آن مطرح می‌شود. همچنین مراکز تحقیقاتی و پژوهشی فعال در این حوزه و پروژه‌های تحقیقاتی مورد توجه آنها بررسی می‌گردد. مراجع استفاده شده برای این گزارش، در ابتدای هر بخش ارائه شده است و در کنار موضوعات مربوطه قرار دارد.

### ۱-۱- هدف

اینترنت اشیاء مفهومی است که اخیرا مطرح شده و توجه بسیاری از شرکت‌های فناور معتبر جهانی مثل اینتل، مایکروسافت، سیسکو، IBM، گوگل و سامسونگ را به خود جلب کرده است. از نگاه اینترنت اشیاء، تمام اشیاء حقیقی و حقوقی محیط اطراف دارای شناسه خواهند بود و در محیطی یکپارچه به تبادل ارتباطات خواهند پرداخت. اینترنت اشیاء، به معنی امکان برقراری ارتباط تمام اشیاء با یکدیگر و با انسان‌ها، به همراه شناسایی و کشف آن‌ها تحت یک شبکه یکپارچه است. طبیعی است که ایجاد چنین شبکه‌ای، مخاطرات فراوانی را به همراه دارد. شبکه جهانی اینترنت که از همگانی شدن آن سال‌ها می‌گذرد، هنوز دارای ضعف‌های امنیتی بسیاری در خود است که موجب به خطر افتادن اموال و حتی جان انسان‌ها نیز شده است. در چنین شرایطی، برقراری امنیت در یک شبکه جهانی از اشیاء که هر کدام با ویژگی‌ها و محدودیت‌های خود به ارتباط با یکدیگر و با انسان‌ها می‌پردازند، طبیعتا از پیچیدگی بسیار بالاتری برخوردار خواهد بود. شرایط جدید محیط و ویژگی‌های مختلف دستگاه‌ها، سبب می‌شود تا امنیت اینترنت اشیاء به طور ویژه مورد توجه قرار بگیرد و معماری‌های متعددی برای آن ارائه شود. همچنین به دلیل وجود بحث

مالکیت اشیاء و همین‌طور حفظ حریم خصوصی افراد، توجه به نکات امنیتی مرتبط با شناسایی و کشف، دسترس‌پذیری، کنترل دسترسی، حریم خصوصی و اعتماد نیز در اینترنت اشیاء از اهمیت بیشتری برخوردار خواهد بود. فناوری اینترنت اشیاء به گونه‌ای است که اگر مورد سوء استفاده قرار بگیرد، حتی امکان به خطر انداختن جان انسان‌ها را دارد و بنابراین می‌توان گفت، امنیت در اینترنت اشیاء یک مبحث کلیدی در اجرایی شدن این فناوری است و به تحقیقات گسترده‌ای جهت حفظ امنیت و حریم خصوصی افراد در این راستا احتیاج است. هدف اصلی این گزارش نیز بررسی امنیت اینترنت اشیاء به عنوان مؤثرترین فناوری نوظهور پس از اینترنت در زندگی انسان‌ها است.

## ۱-۲- ساختار

محتویات این گزارش را می‌توان به ۸ فصل کلّی تقسیم نمود که پس از مقدمه، از فصل دوم، محتویات اصلی گزارش ارائه می‌گردد. در فصل ۲ این گزارش تعاریف و پیشنیازهای لازم برای اینترنت اشیاء بیان می‌شود. به ویژه در این فصل به بررسی کاربردها، مزیت‌ها، پیشران‌ها، بازار فعلی و بازار آینده اینترنت اشیاء می‌پردازیم. در فصل ۳ برخی مراکز تحقیقاتی و پژوهشی مهم در سراسر دنیا در زمینه اینترنت اشیاء، از جمله مراکز پژوهشی، شرکت‌های برتر، دانشگاه‌ها و آزمایشگاه‌ها معتبر مورد بررسی قرار می‌گیرند. در فصل ۴، پروژه‌های امنیتی مهم در زمینه اینترنت اشیاء به طور خلاصه معرفی می‌شوند و معرفی کامل این پروژه‌ها در فاز دوم این گزارش انجام خواهد شد. فصل ۵ به بررسی نیازمندی‌های امنیتی اینترنت اشیاء می‌پردازد. در این فصل نیازمندی‌های امنیت، حریم خصوصی و اعتماد مورد توجه ویژه قرار می‌گیرند و در مورد هر یک توضیحاتی داده می‌شود. در فصل ۶ چالش‌های کلی و چالش‌های امنیتی اینترنت اشیاء به همراه برخی راه‌حل‌های آن‌ها معرفی می‌شوند و در فصل ۷ نیز برخی معماری‌های امنیتی ارائه شده برای اینترنت اشیاء بیان می‌گردند. در نهایت نیز در فصل ۸ یک جمع‌بندی کلی برای گزارش به همراه نتایج بررسی‌ها ارائه شده است. فصل ۹ نیز حاوی واژه‌نامه و مراجع است.

# ۲- تعاریف و پیش‌نیازهای لازم

بررسی حوزه امنیت و پروژه‌های مرتبط با آن در اینترنت اشیاء نیازمند پیش‌نیازهایی جهت آشنایی اولیه با موضوع و روشن شدن اهمیت آن است. به همین دلیل، قبل از ورود به مباحث اصلی، این بخش در نظر گرفته شده تا تعاریف و پیش‌نیازهای لازم برای مطالعه امنیت و حریم خصوصی در اینترنت اشیاء مطرح شوند.

## ۲-۱- تعریف اینترنت اشیاء

ایده اتصال زنجیره‌ای دستگاه‌ها و اشیاء در سطح جهانی با ظهور فناوری RFID مطرح شد. سپس این مفهوم به چشم‌انداز حاضر گسترش پیدا کرد که در آینده نزدیک، با مجموعه بزرگی از اشیاء ناهمگون مواجه خواهیم بود، به طوری که در دنیای فیزیکی با یکدیگر ارتباط برقرار می‌کنند. امروزه، با تشکیل شبکه‌های کوچک، تعداد زیادی از دستگاه‌های همگن قابلیت برقراری ارتباط با یکدیگر را دارند که ما آن را به عنوان "اینترانت اشیاء[۱]" در نظر می‌گیریم. اینترانت اشیاء به معنی برقراری ارتباط داخلی میان اعضای شبکه‌های کوچک مختلف است، اما به دلیل عدم سازگاری، این شبکه‌ها امکان ارتباط با یکدیگر را ندارند. لذا ایجاد یک استاندارد و پروتکل واحد برای برقراری سازگاری این ارتباطات، موجب شکل‌گیری یک شبکه واحد جهانی به نام اینترنت اشیاء خواهد شد.

به طور کلی، به مجموعه استانداردها، پروتکل‌ها، دستگاه‌ها و فناوری‌های لازم برای برقراری ارتباط و انتقال اطلاعات بین دستگاه‌های هوشمند (با یکدیگر و با انسان) در سطح جهانی اینترنت اشیاء (IoT[۲]) گفته می‌شود. از دیدگاه معنایی این مفهوم از ترکیب دو واژه اینترنت و شیء تشکیل شده است. اینترنت یک شبکه گسترده جهانی است که کامپیوترها را بر پایه استانداردهای ارتباطی همچون TCP-IP[۳] به یکدیگر متصل کرده است، و شیء (هوشمند) در این فناوری به صورت یک نهاد مجازی، دیجیتالی یا فیزیکی (هوشمند) تعریف می‌شود که به طور منحصر به فرد قابل شناسایی است. بنابراین اینترنت اشیاء را می توان به صورت یک شبکه بسیار وسیع نیز تعریف کرد که همه اشیاء

---

[۱] Intranet of Things

[۲] Internet of Things

[۳] Transmission Control Protocol - Internet Protocol

موجود در جهان را تحت قواعدی خاص به یکدیگر متصل می‌کند. در واقع، اینترنت اشیاء مفهومی است که در آن اشیاء هوشمند با حسگرها، محرک‌ها[۴]، میکروپروسسورهای کوچک، واسط‌های ارتباطی و منابع انرژی مجهز شده‌اند و قابلیت انجام پردازش‌های متعدد و برقراری ارتباط با یکدیگر را دارند. بنابراین فناوری IoT روش‌های ارتباطی مختلف (مانند RFID، Zigbee، Wi-Fi، 3G/4G/5G)، دستگاه‌های فشرده و حسگرها را با یکدیگر ترکیب می‌کند.

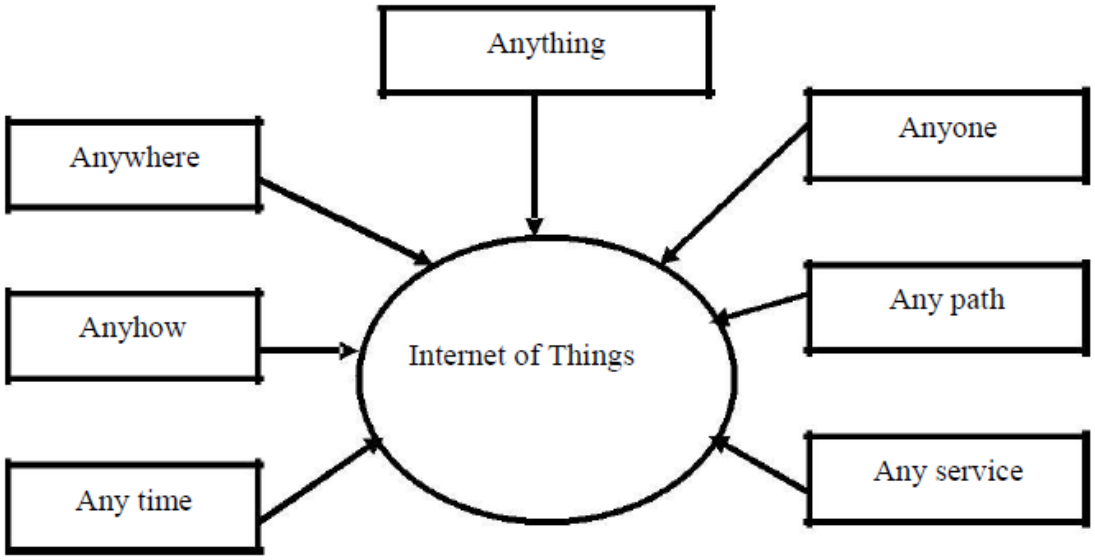
هدف اصلی طراحی این شبکه، به اشتراک گذاردن اطلاعات موجود در هر شیء میان سایر اشیاء مرتبط با آن، در هر زمان و در هر مکان مورد نیاز است. برای اطمینان از اینکه داده‌ها در هر زمان و مکان در دسترس باشند، به پردازش مقدار بسیار زیادی داده جمع‌آوری شده در کاربردهایی مثل نظارت محیط، پیش‌بینی هوا، حمل و نقل، تجارت، سلامت و بهداشت، کاربردهای نظامی و موارد دیگر نیاز است. بنابراین استفاده از یک هسته پردازشی قدرتمند مثل ابر در کنار IoT به وضوح مشخص است و ترکیب شبکه‌های حسگر بی‌سیم با رایانش ابری، اشتراک گذاری و تحلیل آنی اطلاعات حسگرها را ممکن می‌سازد. همچنین مسأله ظرفیت ذخیره‌سازی نیز ممکن است توسط روش‌های کم‌هزینه رایانش ابری پاسخ داده شود که برای ایجاد امنیت و دسترسی آسان به اطلاعات، به صورت گسترده در محیط‌های توزیع شده و موبایل استفاده می‌شود.

### ۲-۱-۱- پارادایم "هر"

شکل ۲-۱-۱-۱ پارادایم "هر"[۵] را نشان می‌دهد. برای ایجاد سرویس‌ها در هر زمان و هر مکان، تعداد زیادی از اشیاء حسگر هوشمند به اینترنت متصل می‌شوند که باید با هویت یکتای خود با یکدیگر ارتباط برقرار کنند. اینجا، جایی است که IPv6 با 128 بیت وارد می‌شود که می‌تواند $2^{128}$ شیء را پشتیبانی کند (که رقم بسیار بزرگی است).

[۴] Actuator

[۵] Any Paradigm




شکل ۲-۱-۱-۱ پارادایم "هر" در IoT

## ۲-۱-۲- برخی حوزه‌های تحقیق و توسعه در اینترنت اشیاء

خلاصه برخی از بخش‌های اساسی که اینترنت اشیاء جهت تحقق اهداف خود در آینده نیاز به توسعه در آن‌ها دارد، به این ترتیب است:

۱- ناهمگونی اشیاء: فناوری IoT قصد دارد تعداد زیادی شیء متفاوت را با قابلیت‌های گوناگون در زمینه ارتباطات و پردازش اطلاعات سازمان‌دهی کند. بنابراین مدیریت چنین مجموعه بزرگی از اشیاء ناهمگون نیاز به یک معماری مناسب و پروتکل‌های ارتباطی کارآمد خواهد داشت.

۲- تبادل اطلاعات: در فناوری IoT، ارتباطات بی‌سیم نقش برجسته‌ای ایفا می‌کند؛ چرا که این نوع از ارتباط باید همه جا در دسترس باشد. بنابراین طراحی ارتباط بی‌سیمی که به لحاظ سرعت و امنیت انتقال اطلاعات، و سهولت و سازگاری استفاده از آن در این فناوری مناسب باشد، بسیار ضروری است.

۳- بهینه‌سازی مصرف انرژی: با توجه به محدودیت منابع انرژی، طبیعی است که بهینه‌سازی مصرف انرژی در ارتباطات میان اشیاء و یا انجام محاسبات آن‌ها یک موضوع اساسی در فناوری IoT است. بنابراین طراحی اشیائی که مصرف انرژی پایینی دارند، در فناوری IoT بسیار مورد توجه قرار دارد.

۴- مدیریت داده: در فناوری IoT همواره باید مقادیر عظیمی داده در حال تغییر و یا آنالیز باشند. بنابراین برای سهولت در تبدیل داده‌ها به اطلاعات و پردازش آن‌ها، باید یک شیوه استاندارد برای آن‌ها تعیین کرد.

۵- حفظ امنیت و حریم خصوصی: از آنجایی که اطلاعات خصوصی همیشه در معرض دستبرد است، بنابراین معماری فناوری IoT باید به نوعی باشد که در مقابل تهدیدات و سرقت اطلاعات خصوصی افراد مقاوم باشد.

### ۲-۱-۳- دسته‌بندی اینترنت اشیاء از دیدگاه‌های مختلف

IoT از دیدگاه‌های مختلف قابل دسته‌بندی است که در این زیربخش، به بیان برخی از آن‌ها می‌پردازیم:

#### ۲-۱-۳-۱-دسته‌بندی کلی برای اینترنت اشیاء

[Zhou Book]

در صورتی که اینترنت اشیاء را ارتباطات دستگاه‌های الکترونیکی با یکدیگر در نظر بگیریم و هر یک از این دستگاه‌ها را یک ماشین بنامیم، از نظر مجله M2M (که در حال حاضر به اسم Connected World شناخته می‌شود) ۶ دسته‌بندی برای ارتباطات ماشین با ماشین (M2M) وجود دارد:

۱- نظارت از راه دور: بخش اصلی کنترل، جمع‌آوری اطلاعات و اتوماسیون در دارایی‌های صنعتی است.

۲- RFID: فناوری جمع آوری اطلاعات که از برچسب‌های[۶] الکترونیکی برای ذخیره اطلاعات استفاده می‌کند

۳- شبکه‌های حسگری: شرایط محیطی یا فیزیکی را با شبکه‌ای از حسگرها نظارت می‌کندپ

۴- سرویس هوشمند: به فرایند شبکه کردن تجهیزات و نظارت روی آن‌ها در سمت مشتری اشاره دارد که امکان نگهداری و سرویس‌دهی کاراتری را فراهم می‌کند.

۵- TELEFMATIC: یکپارچگی مخابرات و انفورماتیک است، اما اغلب به ردیابی، مکان‌یابی و کاربردهای سرگرمی در خودروها اشاره می‌شود.

---

[۶] Tags

۶- TELEMETRY: معمولا وابسته به پزشکی صنعتی و کاربردهای ردیابی که داده‌های بیسیم کمی را منتقل می‌کنند، است.

البته این تقسیم‌بندی، سبب تفکیک مناسبی نمی‌شود و مواردی مثل مدیریت ناوگان[۷] در چند دسته با یکدیگر قرار می‌گیرند. به همین منظور، مرجع [Zhou Book] دسته‌بندی کلی برای اینترنت اشیاء ارائه داده است:

۱- M2M (Internet of Devices): M2M از دستگاه‌های مختلف (مثل حسگرهای خودرو) برای دریافت انواع رویدادها (مثل اختلال در موتور) توسط یک شبکه (بیشتر به صورت شبکه‌های بیسیم سلولار، البته گاهی اوقات سیمی و هیبرید) متصل شده به یک سرور مرکزی (برنامه نرم‌افزاری)، استفاده می‌کند تا رویدادهای جمع‌آوری شده به اطلاعات با معنی تبدیل شوند (مثل هشدار برای تعمیرگاه)

۲- RFID (Internet of Objects): استفاده از امواج رادیویی برای انتقال داده‌ها به یک خواننده[۸]برای اهداف شناسایی و ردیابی شیء

۳- WSN (Internet of Transducers): شبکه‌های حسگری شامل مجموعه حسگرهای خودمختار توزیع شده از نظر مکانی است تا شرایط فیزیکی و محیطی مثل دما، فشار، حرکت، یا آلودگی را نظارت کنند و با مشارکت با یکدیگر، داده‌های خود را از درون شبکه به یک مکان مرکزی انتقال دهند. این شبکه‌ها بیشتر ساختار مش به صورت بیسیم با برد کوتاه دارند و برخی اوقات سیمی یا هیبرید هستند (اشتراکات و تفاوت‌هایی با شبکه M2M و RFID در WSN هست که در مرجع مورد بررسی به آن پرداخته شده است).

۴- SCADA (Internet of Controllers): یک سیستم خودمختار بر اساس نظریه کنترل حلقه بسته یا یک سیستم هوشمند یا CPS است که تجهیزات را توسط یک شبکه، متصل، کنترل و نظارت می‌کند (بیشتر به صورت سیمی با برد کوتاه و گاهی هم بیسیم یا هیبرید).

---

[۷] Fleet management

[۸] Reader

دسته‌بندی دقیق این چهار دسته و فناوری‌های مجزای شبکه آن‌ها در شکل ۲-۱-۳-۲ و جدول ۲-۱-۳-۱ آمده است.

**جدول ۲-۱-۳-۱ چهار حوزه IoT و ارتباط آن‌ها با یکدیگر**

**Table 3.1 Four Pillars of IoT and Their Relevance to Networks**

| *Four Pillars and Networks* | *Short-Range Wireless* | *Long-Range Wireless* | *Short-Range Wired* | *Long-Range Wired* |
|---|---|---|---|---|
| RFID | Yes | Some | No | Some |
| WSN | Yes | Some | No | Some |
| M2M | Some | Yes | No | Some |
| SCADA | Some | Some | Yes | Yes |

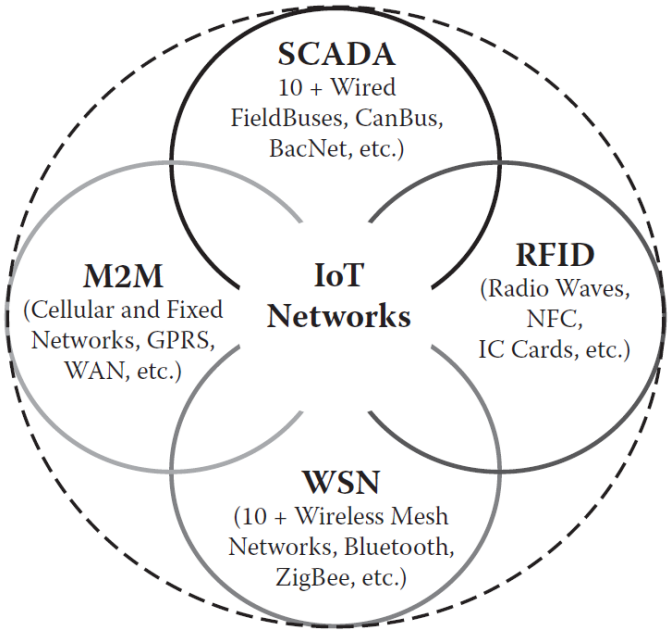



**Figure 3.2 The four pillars of IoT paradigms and related networks.**

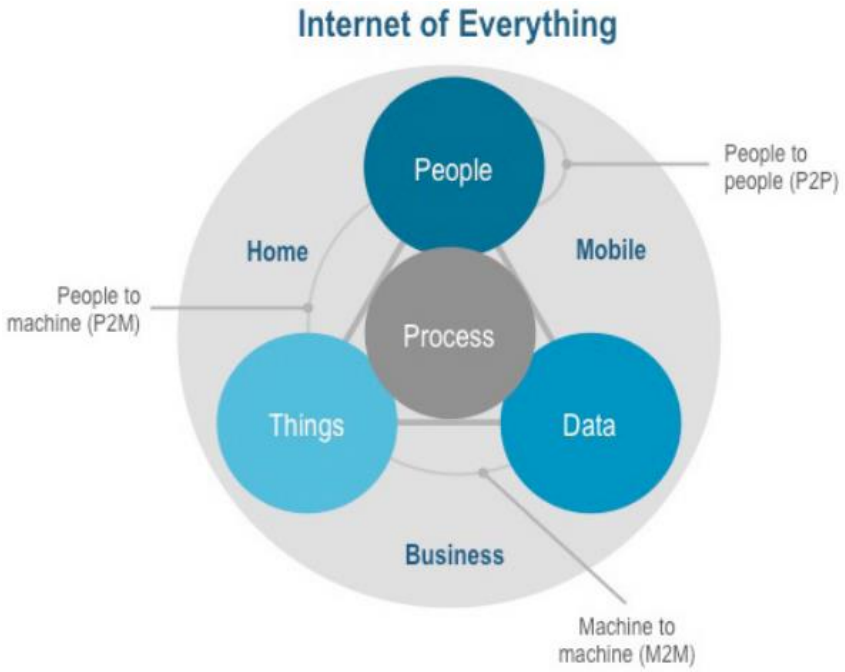
**شکل ۲-۱-۳-۲چهار حوزه IoT و ارتباط آن‌ها با یکدیگر**

نیازمندی‌های امنیتی در این دسته‌بندی‌ها اشتراکات فراوانی دارد، اما اجرایی کردن آن‌ها به دلیل تفاوت در شرایط و محدودیت‌های محیطی و پردازشی، متفاوت می‌شود.

### ۲-۱-۳-۲-دسته‌بندی از دیدگاه Cisco

[everything-for-cities]

شرکت Cisco اجزای IoT را به چهار دسته مردم، فرایند، داده و اشیاء تقسیم‌بندی کرده و ارتباطات میان آن‌ها را نیز با سه مجموعه P2P[۹]، P2M[۱۰] و M2M مشخص می‌کند. شکل ۲-۱-۳-۳ این اجزا و ارتباطات را بهتر مشخص کرده است.




**شکل ۲-۱-۳-۳ اجزا و ارتباطات IoT از دیدگاه Cisco**

در ادامه به صورت مختصر، اجزای IoT از دیدگاه Cisco مورد بررسی قرار می‌گیرد.

- مردم: با اینترنت اشیاء مردم خواهند توانست به شیوه‌های مختلف به اینترنت متصل شوند. امروزه مردم از گوشی هوشمند، کامپیوتر، تبلت و TV برای اتصال به اینترنت و شبکه‌های اجتماعی استفاده می‌کنند. در آینده، برای مثال حتی حسگرهای مورد استفاده توسط یک فرد (مثلا برای اندازه‌گیری پارامترهای سلامت و بهداشت وی) نیز به اینترنت متصل خواهد بود.

---

[۹] People to People

[۱۰] People to Machine

- داده: با IoT، دستگاه‌ها داده‌ها را جمع‌آوری می‌کنند و آن‌ها را توسط اینترنت به یک منبع مرکزی جهت پردازش و تحلیل ارسال می‌نمایند. هرچه قابلیت‌های اشیاء متصل شده به اینترنت افزایش یابد، آن‌ها قادر به استفاده از هوش بیشتر و استخراج داده‌های با ارزش‌تر به منبع خواهند بود و به نوعی، به جای داده، اطلاعات مفید را ارسال خواهند کرد.
- اشیاء: این گروه شامل اشیاء فیزیکی مثل حسگرها(ی هوشمند)، محرک[۱۱]ها و دستگاه‌های مصرف کننده هستند که به یکدیگر و به اینترنت متصلند. در IoT، این اشیاء داده‌های بیشتری را بررسی می‌کنند، از محتوا آگاه خواهند بود و اطلاعات مفیدتری را برای کمک به مردم و ماشین‌ها در تصمیم‌گیری آن‌ها ارائه خواهند داد.
- فرایند: فرایند نقشی کلیدی در چگونگی کار کردن هر کدام از سه نهاد مردم، داده و اشیاء با یکدیگر ایفا می‌کند. با پردازش صحیح، اطلاعات در زمان مورد نظر، به مقصد درست و به بهترین شکل منتقل می‌شود.

## ۲-۲- چشم‌انداز، اهمیت و اهداف

[http://www.gartner.com/newsroom/id/2819918]

[http://www.techtimes.com/articles/31467/20150208/top-5-internet-things-devices-expect-future.htm]

[http://atos.net/content/dam/global/documents/your-business/atos-white-paper-internet-of-things.pdf]

[https://tech.co/internet-of-things-shaping-future-2014-11]

انتظار می‌رود اینترنت اشیاء، انقلاب بعدی باشد که پس از شبکه جهانی وب رخ می‌دهد. ایجاد پلی بین جهان مجازی و دنیای واقعی هدفی است که این فناوری در آینده نزدیک به آن دست خواهد یافت. همین جملات کافی است که برای شناخت این جهان شگفت‌انگیز که به زودی رخ خواهد داد و چه بسا در مناطقی از جهان رخ داده باشد اقداماتی صورت گیرد.

[۱۱] Actuator

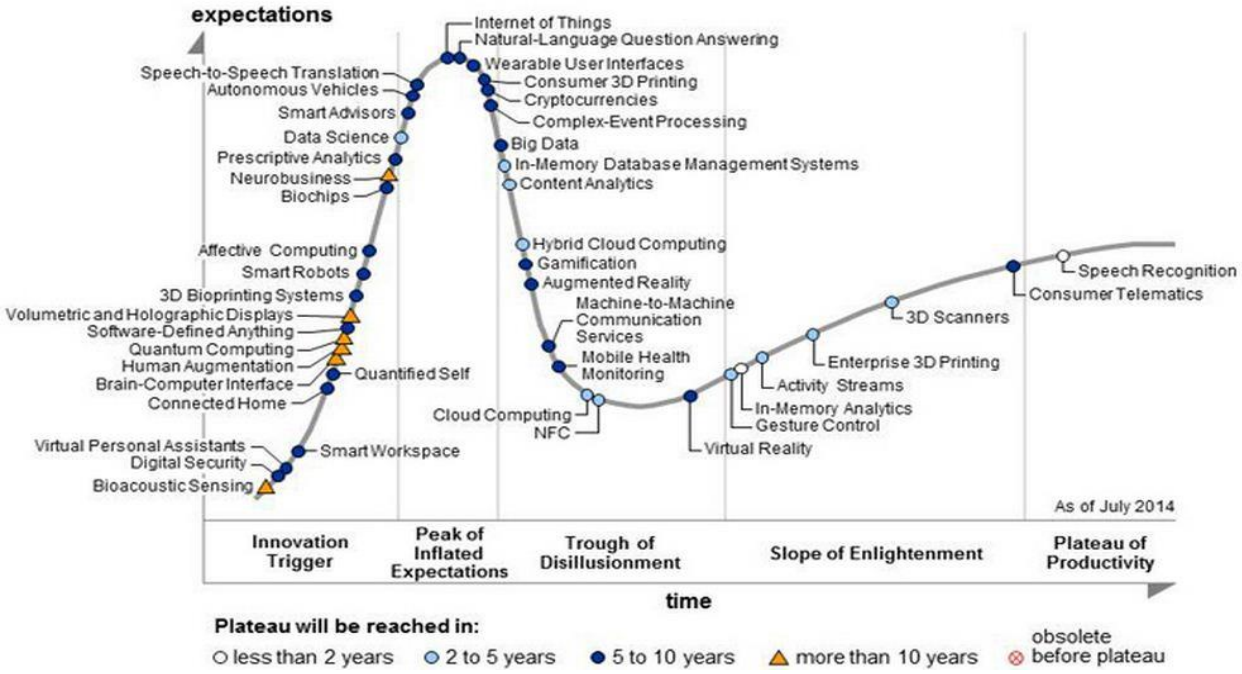
تصور کنید که بعد از یک روز سخت کاری تصمیم دارید با ماشین خود برای استراحت به منزل بازگردید. آخرین چیزی که در این موقعیت می‌خواهید این است که با ترافیک مواجه نشوید. به نظرتان عالی نمی‌شد اگر اتومبیل شما می‌توانست خودش مسیر بهینه و بدون ترافیک تا منزل را برایتان انتخاب کند؟ چنین اتومبیل‌های هوشمندی که می‌توانند به نوعی خودشان حرکت کنند، با استفاده از یک سیستم ارسال سیگنال‌های آنلاین قابل تحقق است. حال فرض کنید که وارد خانه شده‌اید و از قبل دمای هوای اتاق در حد مطلوبی نگه داشته شده و قهوه نیز آماده مصرف است. خانه هوشمند شما یکی از هزاران قابلیتی است که اینترنت اشیاء می‌تواند برای شما ایجاد کند.

اگرچه اینترنت اشیاء هنوز آن‌گونه که انتظار می‌رود تحقق پیدا نکرده است، اما منابع و مشاهدات بسیاری خبر از این می‌دهد که در آینده‌ای نه چندان دور رؤیای حضور این فناوری به واقعیت تبدیل خواهد شد و انقلاب عظیمی که انتظارش را داریم رخ خواهد داد. دو علت اساسی را برای رخداد این انقلاب می‌توان برشمرد:

- کاهش در همه هزینه‌های مصرفی.
- دسترسی نامحدود به همه آنچه که در اطراف ما رخ می‌دهد.

شاید اساسی‌ترین هدف IoT را بتوان اتصال دنیای فیزیکی با دنیای دیجیتال دانست. IoT کمک می‌کند تا بتوانیم شبکه‌ای یکپارچه از میلیاردها شئ با قابلیت اتصال بی‌سیم داشته باشیم تا در صورت لزوم با یکدیگر تبادل اطلاعات داشته باشند. این دورنما، دنیای جدیدی را نشان می‌دهد که در آن اشیاء هوشمند می‌توانند در کنترل همه اتفاقات به کمک بشر بیایند و زندگی را به سطح جدیدی از آن ارتقاء دهند. اشیاء با استفاده از قطعات مخابراتی کوچکی که به آن‌ها متصل است می‌توانند در هر مکان و هر لحظه‌ای مدیریت شوند تا از تخریب یا سرقت آن‌ها جلوگیری به عمل آید. کنتورهای هوشمند برق می‌توانند با کنترل مصرف انرژی علاوه بر این که به کاهش هزینه‌ها کمک کنند، مانع آسیب به منابع انرژی شوند. امروزه پیشرفت‌های فناورانه این دورنما را به واقعیت نزدیک‌تر کرده است.

در شکل ۲-۲-۱-۱ نموداری را مشاهده می‌کنیم که تحت عنوان چرخه هایپ گارتنر[۱۲] معروف است. این نمودار نقشه راه فناوری‌های نو ظهوری را می‌دهد که دنیای دیجیتال را متحول خواهند کرد. همان‌طور که در نمودار نیز مشاهده می‌شود IoT در قله این نمودار (با تخمین ۵ تا ۱۰ سال برای تحقق) قرار دارد.




**شکل ۲-۲-۱-۱ چرخه هایپ گارتنر (نقشه راه فناوری‌های نو ظهور)**

### ۲-۲-۲- مزیت‌ها

هر فناوری روی صنعت تأثیر گذار است و لذا IoT نیز از این قاعده مستثنی نیست. در واقع شیوه جدیدی از مدیریت که IoT با خود به همراه دارد باعث می‌شود کارخانجات و صنایع مختلفی، اقدام به بهره‌برداری از آن کنند. IoT با ارتباطات گسترده و لحظه‌ای که بین انسان و همه اشیاء اطرافش ایجاد می‌کند شکل جدیدی از زندگی را برای او رقم می‌زند. در حقیقت هیچ محدودیتی برای چیزهایی که می‌تواند زمانی به اینترنت وصل باشد وجود ندارد. هم اکنون مثال‌های زیادی از این نوع ارتباط وجود دارد: دستشویی‌های فرودگاه هیترو لندن که میزان استفاده از آن‌ها را گزارش می‌دهند، دویچه تلکام و شرکت آی‌تی فرنچ مدریا[۱۳] یقه‌هایی برای گاوها درست کرده‌اند که دارای ارتباط

[۱۲] Gartner's Hype Cycle

[۱۳] Medria

بی‌سیم برای اتصال به اینترنت است تا از میزان سلامتی گاوها به طور لحظه‌ای باخبر شد، دانش‌آموزان مدرسه‌ای در سامرست (Summerest) با استفاده از اینترنت اشیاء توانستند رشد ارکیده را مشاهده کنند و هزاران مثال دیگری که همگی بیان کننده میزان بهره‌وری از این فناوری گسترده است.

در ابتدای امر لازم است که با مفهوم شئ متصل در IoT آشنا شویم. تأکید می‌شود که خود IoT گاهی اوقات تحت عنوان شبکه ارتباطی بین همه اشیاء که در بستر اینترنت رخ می‌دهد نیز شناخته می‌شود. در IoT هر وسیله می‌تواند به وسیله دیگر برای استفاده از اطلاعات آن و یا دادن اطلاعاتی به آن وسیله وصل شود. حتی برخی از وسایل مجهز به رایانه‌های کوچکی شده‌اند که می‌توانند اطلاعات دریافتی را همزمان پردازش و تحلیل نیز بکنند. در واقع اینترنت اشیاء پلی است بین جهان واقعی و جهان اینترنت: وقتی یک شئ به اینترنت وصل می‌شود پل بین این دو جهان را ایجاد می‌کند. هر وسیله‌ای می‌تواند در دو حالت فعال[۱۴] و یا غیرفعال[۱۵] به اینترنت وصل شود.

در وضعیت غیرفعال، شئ کد شناسایی اش را انتقال می‌دهد. به عنوان مثال بارکد، تراشه RFID و یا هر قطعه دیگری که توسط ماشین قابل خواندن باشد به عنوان کد شناسایی شناخته می‌شود. این اشیاء خودشان مستقیم به اینترنت متصل نیستند، بلکه با استفاده از یک بارکدخوان که کد شئ را شناسایی می‌کند، این اطلاعات می‌توانند در بستر اینترنت منتشر شوند. در واقع فایده اصلی این ارتباط، اطلاع از میزان اشیاء موجود در یک مکان است که در ادامه خواهیم دید برای خرده‌فروشان بسیار کارآمد خواهد بود.

در وضعیت فعال، شئ با استفاده از تکنولوژی که در ساختارش قرار گرفته می‌تواند به طور مستقیم به اینترنت برای ایجاد ارتباط متصل شود. به عنوان مثال می‌توان از حسگرها، نمایش‌دهنده‌ها[۱۶]، درگاه‌ها[۱۷] و محرک‌ها[۱۸] نام برد. حسگرها این قابلیت را دارند که مقداری ( مانند مکان، دما، کیفیت هوا، سرعت و ...) را اندازه گیری کنند و آن را در خود ذخیره یا همزمان ارسال کنند. نمایش دهنده‌ها برای نمایش اطلاعات به انسان با استفاده از صفحه نمایش، نور

---

[۱۴] Active mode

[۱۵] Passive mode

[۱۶] Presenters

[۱۷] Gateway

[۱۸] actuators

پایه و یا صدا به کار می‌روند. به عنوان مثال حسگر سرعت و یا مکان در یک اتومبیل می‌تواند اطلاعات سرعت اتومبیل را بخواند و آن‌ها را برای اتومبیل دیگر ارسال کند. با استفاده از نمایش دهنده‌ها می‌توان راننده را آگاه کرد که اتومبیل جلویی در حال افزایش یا کاهش سرعت خود است. درگاه‌ها نقش ایجاد ارتباط بین وسایل را ایفا می‌کنند. محرک‌ها با استفاده از دستوراتی که از طریق درگاه‌ها و در بستر اینترنت دریافت می‌کنند، می‌توانند حالت یا وضعیت جسم را تغییر دهند.

قطعا یک شئ فعال می‌تواند کاربری‌های بیشتری نسبت به آنچه که برشمردیم داشته باشد. به عنوان مثال در شبکه حسگرها، هر حسگر می‌تواند خود یک درگاه باشد، به همراه قابلیت ارتباط با بقیه حسگرها در ایجاد یک شبکه اقتضایی[۱۹]، برای اینکه ارتباط اینترنتی ساده‌تر و ارزان‌تری فراهم شود.

اشیاء متصل میزان زیادی از اطلاعات را تولید می‌کنند که باید ذخیره، پردازش و یا منتقل شوند. اگر گذشته داده‌ها نیز لازم باشد ذخیره شود با مشکل حجم عظیمی از پایگاه‌های داده مواجه می‌شویم. در اینجا فرصت مناسبی در زمینه‌های جمع‌آوری و حق‌الزحمه پایگاه‌بندی این داده‌ها ایجاد می‌شود. با پیشرفت‌های اخیر در زمینه محاسبات ابری، راه‌حل‌های بسیاری برای جمع‌آوری و پردازش این حجم از اطلاعات داده شده است. پلتفرم‌هایی که می‌توانند کارگذاری این حجم از اطلاعات را انجام دهند، چیزی است که دانش امروزی بشر به آن دست یافته است. علاوه بر این شاهد هستیم که ظهور IoT و نیاز آن به پردازش سریع اطلاعات باعث پیشرفت در زمینه‌های دیگر مانند محاسبات و رایانه‌های کوانتومی شده است.

ادغام و به هم پیوستگی وسایل هوشمند نقش حیاتی در IoT بازی می‌کند. برای شرکت‌های بزرگ آی‌تی در دنیا این یک فرصت استثنایی است تا پلتفرم‌هایی را به بازار ارائه دهند که دارای قابلیت‌های زیر باشد:

- پشتیبانی از پروتکل‌ها و استانداردهای مختلف ارتباطی که در فرکانس‌های مختلفی کار می‌کنند.
- به معماری‌های مختلف اجازه انتشار و یا تمرکزدهی را بدهند.
- امکان ارتباط با شبکه‌های دیگر را داشته باشند.

[۱۹] Ad-hoc

- دارای قابلیت خدمت‌رسانی لحظه‌ای باشند.

در نهایت به صورت کلی، به نقش IoT در زمینه‌های مختلف می‌پردازیم که هر یک از زمینه‌ها در ادامه گزارش به صورت دقیق‌تر مورد بررسی قرار خواهد گرفت. اینترنت اشیاء بر روی همه ساختارها و ارگان‌های کاربری، از محیط زیست گرفته تا بهداشت، ترافیک، تولیدو مصرف انرژی برق و مدیریت شهری تأثیری شگرف خواهد داشت. مزیت‌های استفاده از IoT در همه ساختارهای زندگی انسان مشهود است.

**شهرهای هوشمند:** شهر هوشمند زیرساخت خدمات عمومی و فعالیت‌های تجاری را از طریق ایجاد شبکه‌های ارتباطی، بسیار مکانیزه‌تر می‌کند. حسگرهایی که در سراسر شهر توزیع شده‌اند تا اطلاعات رفتاری انسان‌ها در زمینه مصرف‌کنندگی، استفاده از امکانات و سایر حوزه‌های مرتبط با رفتار اجتماعی را جمع‌آوری کنند. ارگان‌های نظارتی شهر با دریافت این اطلاعات، برای افزایش سطح زندگی افراد ساکن در شهر اقدامات لازم را انجام می‌دهند.

**صنعت حمل‌ونقل:** با ظهور IoT این صنعت دچار تحول بسیاری خواهد شد اما هنوز برای رسیدن به آن سطح از ارتباطات بین اشیاء در صنعت حمل‌ونقل محدودیت‌هایی وجود دارد. به عنوان مثال هنوز دسترسی آنی به اطلاعات ترافیک امکان‌پذیر نیست. با رفع این مشکلات و تبدیل اتومبیل‌ها به وسایلی متصل به اینترنت علاوه‌بر این‌که باعث کنترل ترافیک می‌شود، از بروز بسیاری از تصادفات نیز جلوگیری می‌کند. شرکت گوگل در حال حاضر در حال ساخت اتومبیلی است که می‌تواند تا هزار مایل بدون کمک انسان و تا ۱۴ هزار مایل با کمی کمک از انسان به مسیر خود ادامه دهد.

**بخش هوانوردی:** در بخش هوانوردی، IoT می‌تواند با استفاده از حسگرها، فشار، دما و لرزش هواپیما را اندازه بگیرد و به طور مداوم آن‌ها را کنترل کند. این قابلیت امکان دسترسی لحظه‌ای به اطلاعات هواپیما و شرایط مسافران را هم برای برج مراقبت و هم برای خلبان فراهم می‌کند. تگ‌های RFID که به قطعات هواپیما وصل می‌شوند، می‌توانند مانع از به کار رفتن قطعات قلابی در ساختار هواپیما شوند. حداقل ۲۸ حادثه هوایی در آمریکا ناشی از همین قطعات تقلبی بود.

**بخش انرژی:** در بخش انرژی، IoT می‌تواند به نظارت و مدیریت مصرف انرژی کمک کند. کاربردهای هوشمند باعث می‌شود که علاوه بر عملکرد بهینه در حفاظت از انرژی، بتوان به مصرف‌کنندگان خدمات بهتری ارائه داد.

کنترهای هوشمند با فرستادن سیگنال‌هایی به مصرف‌کنندگان، میزان مصرف آن‌ها را تنظیم می‌کنند. این عمل علاوه بر کاهش هزینه‌های مصرفی در ساعات اوج بار، از قطعی ناشی از افزایش بار نیز جلوگیری می‌کند.

حسگرهایی که در مناطق حساس لوله‌های انتقال گاز نصب شده‌اند، می‌توانند فشار و حجم گاز انتقالی در هر لحظه را اندازه‌گیری کرده و در اختیار متصدیان نظارت بر روند انتقال انرژی قرار دهند تا در لحظات اضطراری، قبل از اینکه حادثه‌ای رخ دهد اقدامات لازم را انجام دهند.

**تولید:** بسیاری از شرکت‌های تولیدی برای نظارت و مدیریت تولیداتشان از برچسب‌های RFID استفاده می‌کنند. این برچسب‌ها علاوه بر اینکه فهرست‌بندی را راحت‌تر می‌کنند، مانع از جعل و تقلب نیز می‌شوند. حسگرهایی که به تولیدات وصل شده‌اند، می‌توانند مصرف کننده را از صحت و سلامت وسیله آگاه کنند. در واقع باید گفت نظارت بر کالا از تولید تا زمانی که به دست مصرف‌کننده می‌رسد، بزرگترین ارمغانی است که IoT برای شرکت‌های تولیدی خواهد داشت.

کاربردها و مزیت‌هایی که IoT برای زندگی بشر خواهد داشت بسیار بیشتر از چند موردی است که در بالا برشمردیم. در بخش‌های آتی خواهیم دید که چگونه IoT در همه قسمت‌های زندگی بشر تأثیری شگرف و بنیادین خواهد داشت. در پایان این بخش به عنوان نتیجه باید بگوییم که اینترنت اشیاء، شیوه ارتباطی که امروزه رایج است و تمرکز بر روی داده‌های انسانی می‌باشد را خواهد شکست. فناوری‌هایی مانند RFID، Wi-Fi، مکان‌یابی لحظه‌ای و شبکه حسگرها باعث می‌شود در آینده، مدیریت طبیعت و اشیاء را به دست خودشان بسپاریم.

## ۲-۳- پیشران‌ها

گسترش IoT در انواع حوزه‌های کاربری، موجب تسهیل و تسریع فرآیندها می‌شود، ضمن اینکه کاهش هزینه را نیز در پی دارد. پیشران‌های اقتصادی IoT توسط مؤسسه مکنزی[۲۰] مورد بررسی قرار گرفته که در بخش ۲-۵- به آن پرداخته می‌شود. همچنین مزیت‌های IoT نیز از دیدگاه شرکت مایکروسافت در بخش ۲-۶- بررسی شده است. در

[۲۰] Mckinsey

این بخش ما به بررسی بازار IoT به عنوان یک پیشران مهم برای حرکت به سوی IoT می‌پردازیم و با بررسی بازار فعلی و بازار آینده آن، گسترش این فناوری را توجیه می‌نماییم.

### ۲-۳-۱- بخش‌های بازار فعلی IoT

[http://iot-analytics.com/iot-market-segments-analysis]

خلاصه مطالب مرتبط با بازار IoT- بزرگترین فرصت در تولید صنعتی- شامل موارد زیر است:

- پتانسیل بازار IoT برای برنامه‌های کاربردی مرتبط با تجارت بیشتر از برنامه‌هایی است که برای مصرف‌کنندکان می‌باشد.
- تولید و سلامت بزرگترین بخش‌های بازار IoT در برنامه‌های کاربردی مرتبط با تجارت هستند.
- صنعت نفت و گاز به عنوان یک زیر بخش از تولید، منجر به تلفیق IoT با بخش انرژی و همچنین برنامه‌های کاربردی در حمل‌ونقل شده است.
- با برنامه‌های کاربردی مصرف کننده، در یک سال آینده، خانه هوشمند به یک بحث داغ در بازار تجارت تبدیل خواهد شد.(ترموستات‌های هوشمند، سیستم‌های امنیتی و یخچال‌ها).

با توجه به آخرین تحلیل‌ها، بازار عمومی IoT به صورت زیر خواهد بود:

- تا سال ۲۰۲۰ برای هر فرد حداقل ۲ دستگاه متصل و یا حتی ۶ دستگاه وجود خواهد داشت.
- فرصت‌های کسب درآمد در حوزه IoT به مراتب نسبت به آنچه اپل، فیس‌بوک و گوگل با هم به فروش می‌رسانند بیشتر خواهد بود.
- تأثیر اقتصادی Iot می‌تواند از ۱۰ سال اقتصاد آلمان پیشی بگیرد.

بر اساس این تجزیه و تحلیل، و نظرسنجی‌های به عمل آمده به تفسیر و بررسی بازار رقابتی در IoT می‌پردازیم.

#### ۲-۳-۱-۱-رویکرد تقسیم‌بندی بازار IoT

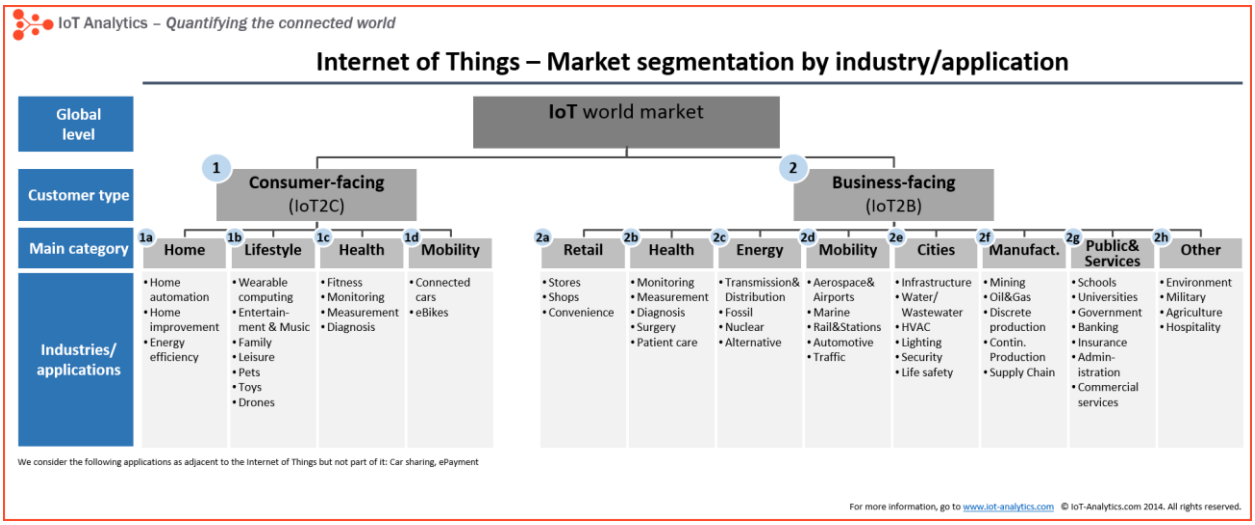
بازار را از سه منظر می‌توان نگاه کرد:

۱- از نقطه نظر کاربرد/صنعت (به عنوان مثال تمایز بین برنامه‌های کاربردی در استخراج معدن و برنامه‌های کاربردی در حمل و نقل)

۲- از نقطه نظر فناوری (به عنوان مثال جدا کردن تولید کنندگان حسگر از ارائه دهندگان راه‌حل تجزیه و تحلیل)

۳- از نقطه نظر جغرافیا (یعنی تمایز بین اروپا و آمریکا)

در این قسمت فقط به تجزیه و تحلیل با استفاده از رویکرد اول خواهیم پرداخت. تقسیم‌بندی بازار جهانی IoT مطابق شکل ۲-۳-۱-۱ است.




**شکل ۲-۳-۱-۱ تقسیم‌بندی بازار جهانی IoT**

تقسیم‌بندی بازار IoT به دو دلیل ارائه می‌شود:

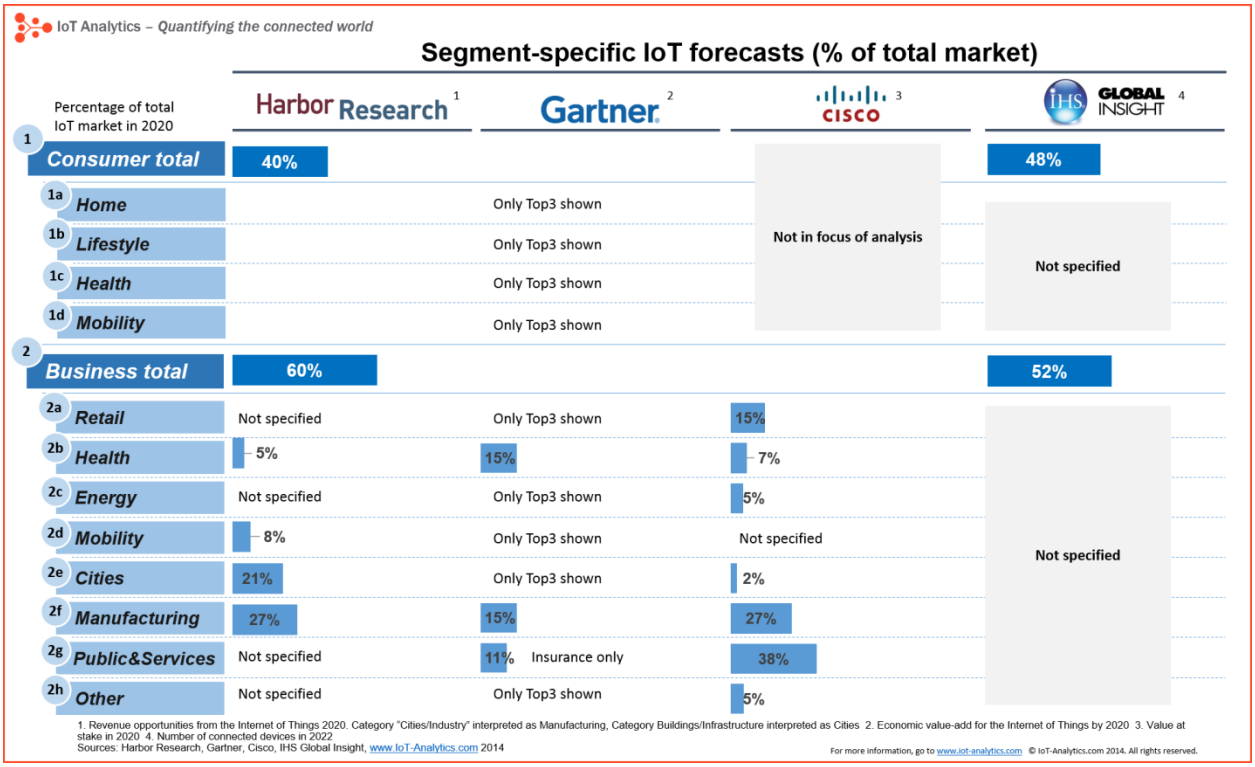
۱- تجارت و مصرف کنندگی را در Iot متمایز می‌کند. شرکت‌هایی که در بخش مصرف کننده IoT فعالیت می‌کنند، مانند تولید کنندگان پوشیدنی‌ها، به دلیل تفاوت در مشتریانشان، همپوشانی بسیار کمی با شرکت‌های صنعتی IoT مانند سیسکو دارند.

۲- همچنین بخش‌های اصلی که اهمیت و تفاوت زیادی با یکدیگر دارند را معرفی می‌کند.

ابتدا پیش‌بینی بخش‌های بازار ، پس از آن بررسی و در نهایت مثال‌های عملی برای کاربردهای مهم ارائه خواهد شد.

### ۲-۳-۱-۲-پیش‌بینی بخش‌های بازار IoT: تولید بزرگترین

۴ گزارش عمومی ارائه شده است که سعی در پیش‌بینی درآمد یا توسعه خاص در هر بخش دارد. اطلاعات مرتبط با این ۴ گزارش در شکل ۲-۳-۱-۲ آمده است.




**شکل ۲-۳-۱-۲ ۴ گزارش عمومی ارائه شده برای پیش‌بینی بازار IoT**

**تفسیر اعداد:**

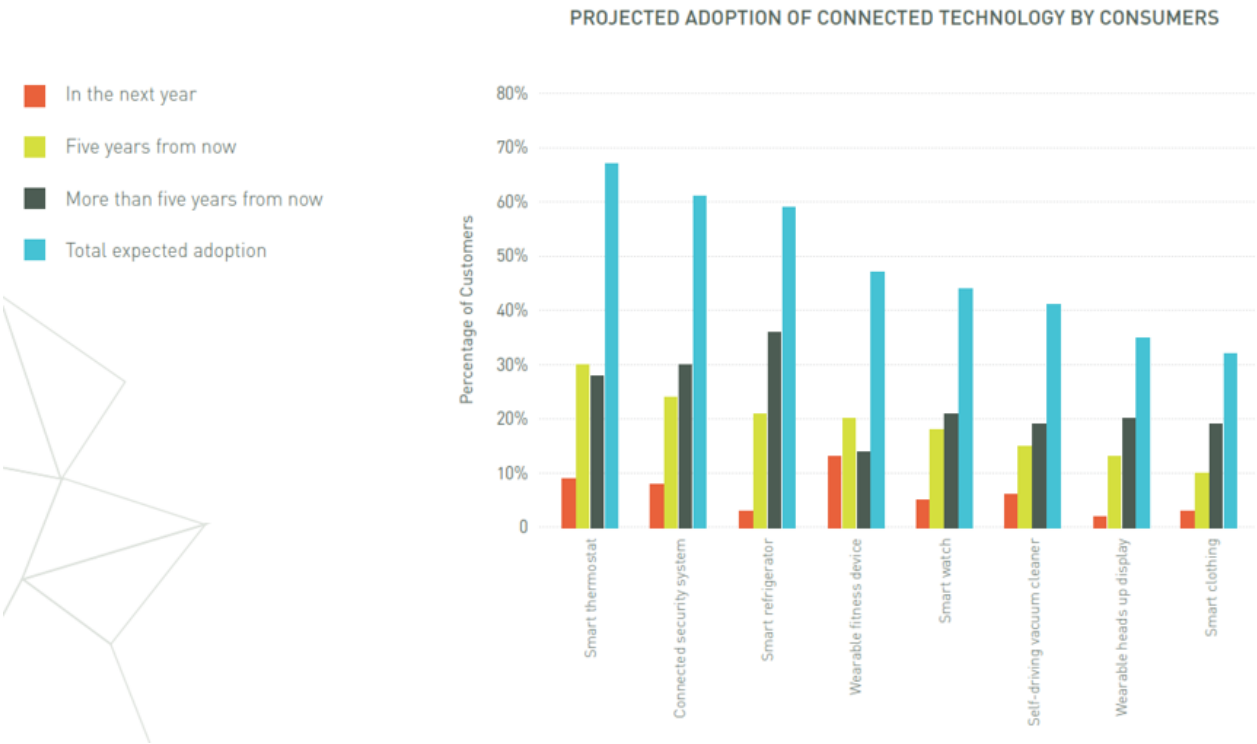
- پتانسیل IoT در برنامه‌های کاربردی تجارت بیشتر از برنامه های مصرف کننده (۵۵ درصد در مقابل ۴۵ درصد) است.
- تولید ظاهراً بزرگترین بخش از IoT (به طور باالقوه بیشتر از ۲۵ درصد کل بازار) خواهد بود.
- بهداشت و درمان بحث مهم دیگر است.(به طور بالقوه بین ۵ تا ۱۵ درصد از کل بازار IoT)
- نظرات بسیار متفاوتی در مورد پتانسیل خدمات عمومی و تجاری وجود دارد.

### ۲-۳-۱-۳- بررسی بخش‌های بازار IoT

علاوه‌بر پیش‌بینی‌های بازار در حال توسعه، بررسی‌ها نشان می‌دهند که در چه قسمت‌هایی پول سرمایه‌گذاری شده و چه صنعت یا کاربردی حاصل شده است.

#### ۲-۳-۱-۳-۱- مصرف کننده IoT: "خانه هوشمند" از کاربردهای با بالاترین تصویب طرح

تنها مطالعه‌ی قابل توجه روی بخش مصرف کننده IoT، اخیراً توسط گروه آکوییتی[۲۱] انجام شده است. این شرکت از بیش از ۲۰۰ مصرف کننده در ایالات متحده نظرسنجی کرده است تا فناوری‌های متفاوت در طول ۵ سال آینده را تصویب کند (شکل ۲-۳-۱-۳).




شکل ۲-۳-۱-۳ پذیرش فناوری توسط مصرف‌کنندگان

[۲۱] Acquity

**تفسیر اعداد:**

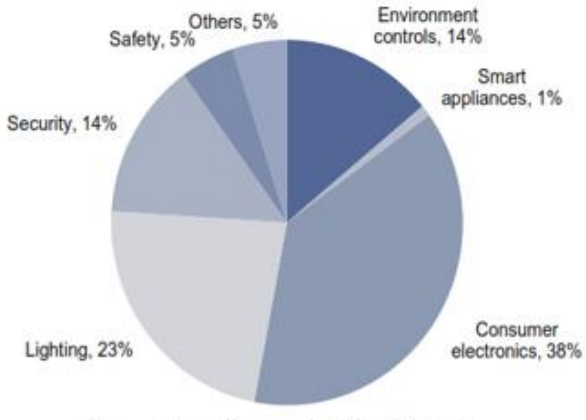
- دستگاه‌های تناسب اندام پوشیدنی که در حال حاضر بر شیوه زندگی مصرف کننده تسلط دارند، بیشتر مورد توجه واقع می‌شوند.
- کاربردهای خانگی بر بازار IoT در چند سال آینده چیره خواهند شد (ترموستات‌های هوشمند، سیستم‌های امنیتی و یخچال‌ها)

متأسفانه در این نظرسنجی برنامه‌های سلامت مصرف کننده مانند نظارت بر سلامت از راه دور، رأی نیاوردند.

**تحلیل بیشتر جزئیات**

**خانه هوشمند:** از زمانی که نست[۲۲] پیش از سال ۲۰۱۴، توسط گوگل ارائه شد، مردم از خانه هوشمند مطلع شدند. گلدمن ساچز[۲۳] پیش‌بینی کرد که لوازم الکترونیکی به صورت عمده توسط مصرف کننده‌ها استفاده خواهد شد (شکل ۲-۳-۱-۴).

**Exhibit 7: Energy efficiency, home comfort and security will be key areas of Industrial focus**




Home automation market - North America

*Source: ABB, Goldman Sachs Global Investment Research*

[۲۲] Nest

[۲۳] Goldman sachs

شکل ۲-۳-۱-۴ بازار خانه هوشمند

شرکت هلندی فیلیپس[۲۴] یکی از اولین مصرف کنندگان لامپ‌های متصل به اینترنت بود. لامپ چراغ برق آن‌ها که HUE نامیده می‌شد حدود ۲۰۰ دلار امروز ارزش داشت. انتظار می‌رود که این قیمت در آینده کاهش شدیدی پیدا کند. پیش‌بینی می‌شود که تا سال ۲۰۲۰ لامپ‌های LED متصل به اینترنت از تنها ۲ میلیون به ۱۰۰ میلیون عدد برسد.

**شیوه زندگی:** در رابطه با پوشیدنی‌ها[۲۵]، جانیپر[۲۶] پیش‌بینی کرده است که میزان استفاده از آن‌ها، از ۱۴ میلیون در سال ۲۰۱۴ به ۱۴۰ میلیون در سال ۲۰۱۸ خواهد رسید. گزارش‌های اخیر مشخص می‌کنند که شرکت‌های پوشیدنی همچون جابن[۲۷] و فیت‌بیت[۲۸] سهام زیادی را از آن خود کرده‌اند.

### ۲-۳-۱-۳-۲- تجارت IoT: انرژی، حمل‌ونقل و تولید

بررسی‌های بسیاری در بازار تجارت IoT انجام شده است. برخلاف پیش‌بینی‌های بازار، این بررسی‌ها بخش‌های متفاوت بازار را رتبه‌بندی نمی‌کنند. به منظور تسهیل تفسیر آن‌ها، بررسی‌ها در شکل ۲-۳-۱-۵ رسم شده است.

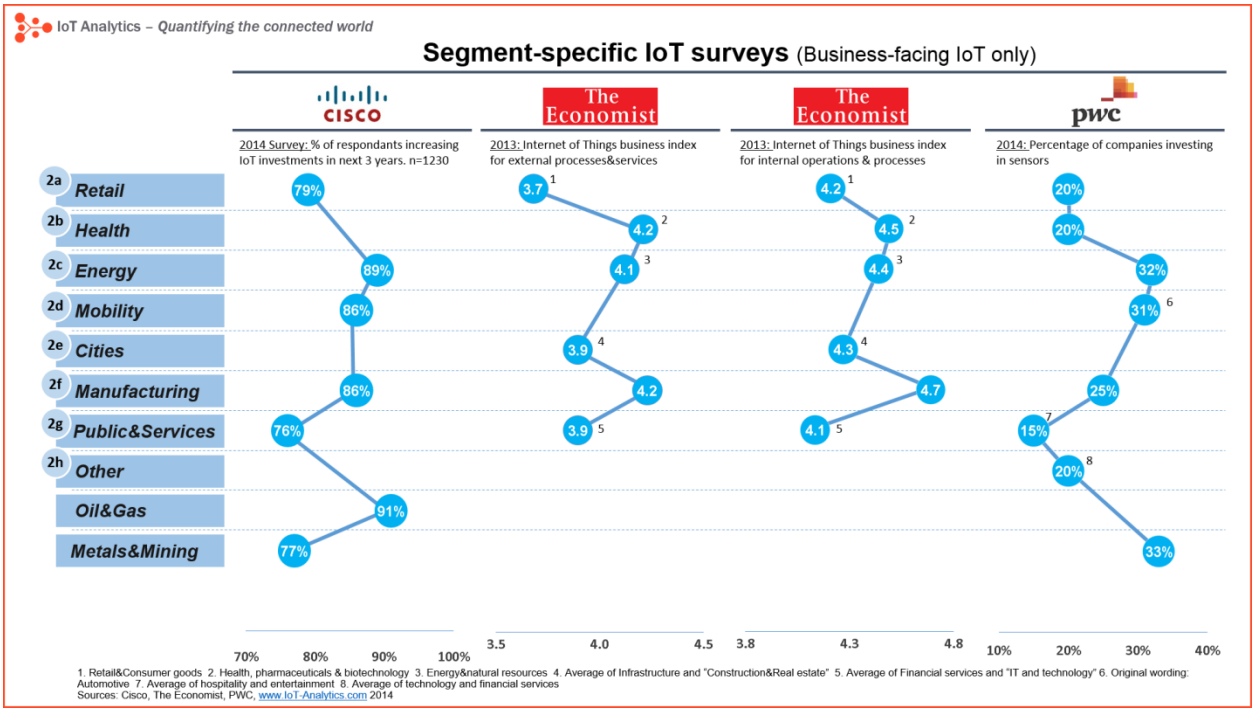
[۲۴] Philipps

[۲۵] Wearable

[۲۶] Juniper

[۲۷] Jawbone

[۲۸] Fitbit




شکل ۲-۳-۱-۵ بررسی تقسیم‌بندی بازار IoT

**تفسیر اعداد:**

- به طور مداوم، انرژی، حمل‌ونقل و تولید، راهنمای سرمایه‌گذاری در حوزه IoT هستند.
- آخرین بررسی سیسکو، صنعت نفت و گاز را به عنوان یک صنعت کلیدی در تولید نشان می‌دهد که در حال حاضر سرمایه‌گذاری در آن در حال افزایش است.
- بخش عمومی و خدمات تجاری مانند خدمات مالی، پشتیبان سرمایه‌گذاری در Iot هستند.
- بخش‌های بازار مختلف IoT همچون بهداشت و درمان و یا فلزات و استخراج کاملا متفاوت هستند. به عنوان مثال در حالی که PWC[۲۹] علاقه کمتری برای سرمایه‌گذاری در سلامت و بهداشت می‌بینند، بیشترین میزان علاقه‌مندی در سرمایه‌گذاری در حوزه فلزات و معدن را انجام می‌کند.

**تحلیل بیشتر جزئیات**

[۲۹] PricewaterhouseCoopers

**انرژی:** یکی از موضوعات بزرگ در انرژی، شبکه‌های هوشمند توزیع و کنتورهای هوشمند هستند. نویگنت[۳۰] پیش‌بینی می‌کند که استفاده از کنتور هوشمند در سال ۲۰۱۸ به اوج خود می‌رسد. انتظار می‌رود که درآمد حاصل از کنتور هوشمند از ۴,۴میلیارد دلار به ۷,۴میلیارد دلار در سال ۲۰۱۸ برسد.

**حمل‌ونقل:** اتومبیل‌های متصل یک کاربرد بزرگ در بخش حمل‌ونقل هستند. شرکت IHS پیش‌بینی می‌کند که تا سال ۲۰۲۰، ۱۵۲ ملیون خودرو به اینترنت متصل خواهد شد.

**تولید:** جای تعجب نیست که دو نفر از سخنرانان کلیدی در انجمن جهانی IoT که اخیراً در شیکاگو برگزار شد از صنعت نفت و گاز و شرکت‌های استخراج معدن بودند. مک گا[۳۱] رئیس نوآوری در ریو تینتو[۳۲] و آرجن دورلند[۳۳] مدیر فنی و رقابتی در شل[۳۴] پتانسیل عظیم IoT را در صنایع خود برجسته کرده‌اند. توانایی IoT برای کنترل از راه دور امکان بزرگی است که آن را برای صنایع مفید می‌سازد.

### ۲-۳-۲- پیش‌بینی بازار آینده IoT

[http://iot-analytics.com/iot-market-forecasts-overview]

در سال ۱۹۴۳، مدیر عامل شرکت IBM[۳۵]، توماس واتسون، پیش‌بینی کرد "یک بازار جهانی برای شاید ۵ کامپیوتر وجود دارد". بیانیه‌ای که به زودی ثابت خواهد شد اشتباه است. خوشبختانه، روش‌های پیش‌بینی در طول ۷۰ سال گذشته بهبود یافته است. این روزها پیش‌بینی کمتر به عنوان یک هنر، بلکه بیشتر به عنوان یک علم شناخته می‌شود. استفاده از روش‌های آماری و شاخص‌های اقتصادی به یک استاندارد گسترده تبدیل شده است.

---

[۳۰] Nevigant

[۳۱] McGagh

[۳۲] Rio Tinto

[۳۳] Arjen Dorland

[۳۴] Shell

[۳۵] IBM

در پیش‌بینی نوآوری‌های فناوری از چشم‌انداز سال ۲۰۱۴، IoT در حال پیشی گرفتن از سایر پیش‌بینی‌هاست. سرفصل‌های پیش بینی شبیه موارد زیر هستند.

- ۵۰ میلیارد دستگاه تا سال ۲۰۲۰ متصل خواهند شد.
- بازار IoT تا سال ۲۰۲۰ تبدیل به یک بازار چند تریلون دلاری خواهد شد.

مقدار دقیق برآوردها و اعداد در بازار IoT بسیار گیج کننده است. با این حال فهم این ارقام به منظور رسیدن به یک حس پویایی از صنعت مهم است. درواقع، تجارت های کوچک و بزرگ و نیز افراد شخصی با استفاده از این پیش‌بینی‌ها به تصمیم گیری‌های مهم در مورد سرمایه‌گذاری، توسعه محصول و غیره می‌پردازند.

در این مقاله همه پیش‌بینی‌های بزرگ مرتبط با بازار IoT را خلاصه شده و تجسم آن‌ها روشن‌تر شده است.

### ۲-۳-۲-۱-شاخص‌های بازار IoT: چه چیزی باعث پیش‌بینی می‌شود

اندازه بازار IoT براساس چهار معیار مهم، اندازه‌گیری می‌شود:

۱- تعداد دستگاه‌های متصل (بر حسب واحد میلیارد اندازه‌گیری می‌شود)

۲- درآمد تولید شده از طریق IoT (برحسب میلیارد دلار اندازه‌گیری می‌شود)

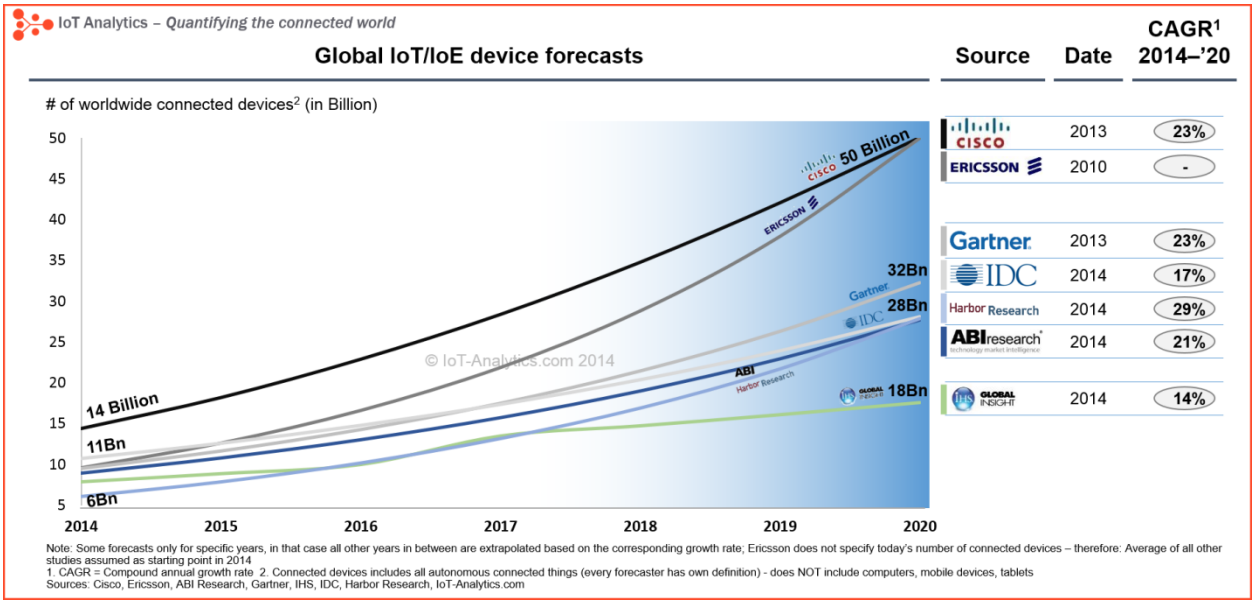
۳- ارزش کل اقتصادی IoT (برحسب تریلون دلار اندازه‌گیری می‌شود)

۴- مقدار ترافیک IP (بر حسب اگزابایت در هر ماه اندازه‌گیری می‌شود)

در اینجا قصد ورود به ترافیک IP را نداریم. ترافیک IP وجود دارد ولی برای بیشتر مردم نا محسوس است. علاوه بر این، به شدت وابسته به تعداد دستگاه‌های متصل است و اهمیت کمتری برای فهم بازار دارد.

### ۲-۳-۲-۲- تعداد دستگاه‌های متصل

سیسکو[۳۶] و اریکسون[۳۷] مقالاتی در مورد بازار آینده IoT منتشر کرده‌اند. هر دو بیش از حدود ۵۰ میلیارد وسیله متصل را پیش‌بینی کرده‌اند. علاوه بر این، شرکت‌های پژوهش بنیان گارتنر[۳۸]، ABI و نیز IDC مراکز تحقیقاتی خود را جهت پیش‌بینی‌های خود در حوزه IoT توسعه داده‌اند (شکل ۲-۳-۲-۱).




شکل ۲-۳-۲-۱ تعداد دستگاه‌های متصل شده

ما امروزه تقریبا بین ۶ تا ۱۴ میلیارد دستگاه متصل و مستقل داریم که از طریق یکی از انواع روش‌های ارتباطات متصل می‌شوند. این ارقام شامل گوشی‌های هوشمند، تبلت‌ها، کامپیوترها، و وسایل مشابه آن‌ها نیست. تعاریف دقیق شرکت‌های پژوهشی کمی متفاوت هستند.

**وجه مشترک پیش‌بینی‌ها:**

[۳۶] Cisco

[۳۷] Ericsson

[۳۸] Gartner

- در سال‌های آینده تعداد دستگاه‌های متصل افزایش زیادی خواهد داشت. پیش‌بینی می‌شود که نرخ رشد آن‌ها نسبت به سایر صنایع فراتر باشد. (نرخ رشد سالانه از ۱۴ درصد به ۲۹ درصد) برای هر فرد زنده بر روی زمین حداقل ۲ و شاید حتی ۶ شئ متصل تا سال ۲۰۲۰ وجود خواهد داشت.
- تا سال ۲۰۲۰ اشیاء بیشترین میزان دستگاه‌های متصل را نشان خواهند داد. امروزه تعداد وسایل متصل که شئ نیستند (مانند گوشی‌های هوشمند، کامپیوترها، تبلت‌ها و غیره) تقریباً برابر تعداد اشیاء متصل است (به عنوان مثال ABI می‌گوید امروزه حدود ۷ میلیارد گوشی هوشمند و کامپیوتر و مشابه آن وجود دارد).

**اختلاف پیش‌بینی‌ها:**

- تعداد دستگاه‌های متصل تا سال ۲۰۲۰. پیش‌بینی کم حدود ۱۸میلیارد و پیش‌بینی سرسختانه حدود ۵۰ میلیارد دستگاه متصل را نشان می‌دهد. باید توجه داشت که اگر سیسکو و اریکسون بالاترین برآورد را ارائه می‌دهند، علتش علاقه آن‌ها برای رسیدن به این عدد است. هر دو در حال فروش راه‌حل در زمینه IoT و شرطبندی روی این صنعت هستند.

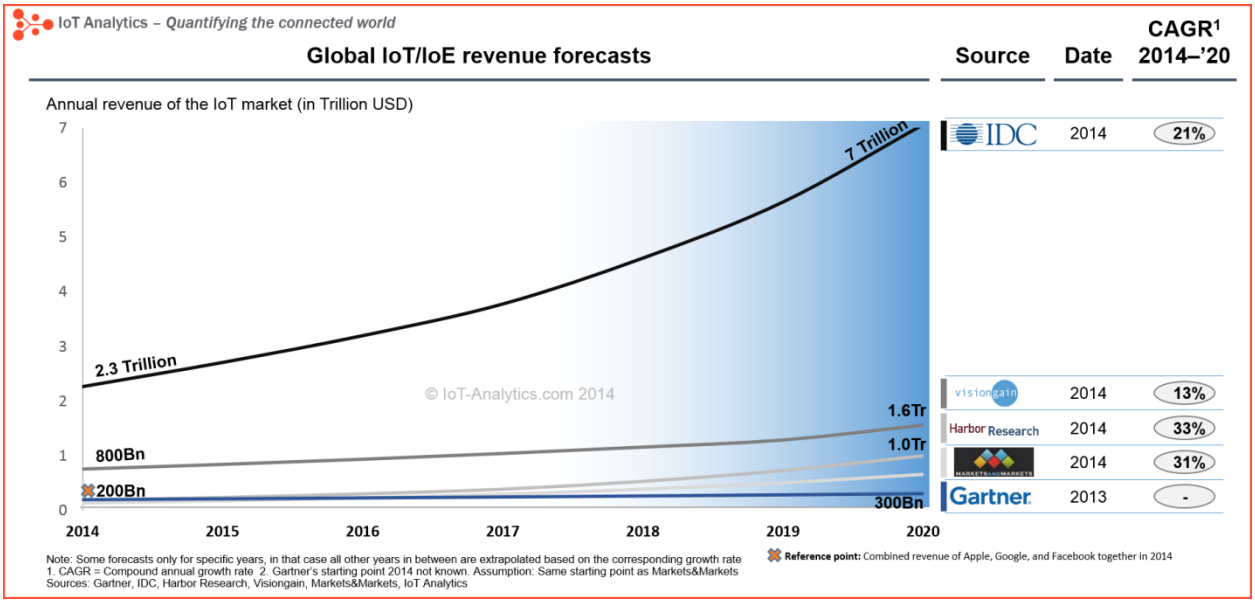
شرکت‌های پژوهشی جهت ارزیابی این بازار، روش مدلسازی سنتی از بالا به پایین را انجام داده‌اند. به عنوان مثال گارتنر پیش‌بینی‌هایش را با استفاده از سه روش مختلف بیان می‌کند: تجزیه و تحلیل محصولات با دنباله طولانی[۳۹]، مطالعه تعداد در هر جامعه و یک تجزیه و تحلیل اقتصادی

سیسکو با این حال یک رویکرد متفاوت در پیش گرفته است. این شرکت صنعت را به طور کامل از پایین تا بالا اندازه می‌گیرد و ۵۰ مورد استفاده از IoT را در بخش خصوصی تجزیه و تحلیل می‌کند.

[۳۹] Long-Tail Product Category

### ۲-۳-۲-۳- درآمد[۴۰] کسب شده

۵ شرکت IDC[۴۱]، ویژن‌گین[۴۲]، هاربورریسرچ[۴۳]،مارکتس اند مارکتس[۴۴] و گارتنر، چگونگی افزایش درآمد از طریق شرکت‌های فعال در حوزه IoT را برآورد می‌کنند (شکل ۲-۳-۲-۲).




**شکل ۲-۳-۲-۲ پیش‌بینی درآمد جهانی حاصل از IoT/IoE[۴۵]**

**وجه مشترک پیش‌بینی‌ها:**

- ما یک افزایش عظیم در درآمد حاصل از IoT در سال‌های آینده خواهیم داشت که با رشد دو رقمی تولید همراه است.

**اختلاف پیش‌بینی‌ها:**

---

۴۰ Revenue

۴۱ IDC

۴۲ Visiongain

۴۳ Harbor Research

۴۴ Markets&Markets

۴۵ Internet of Everything

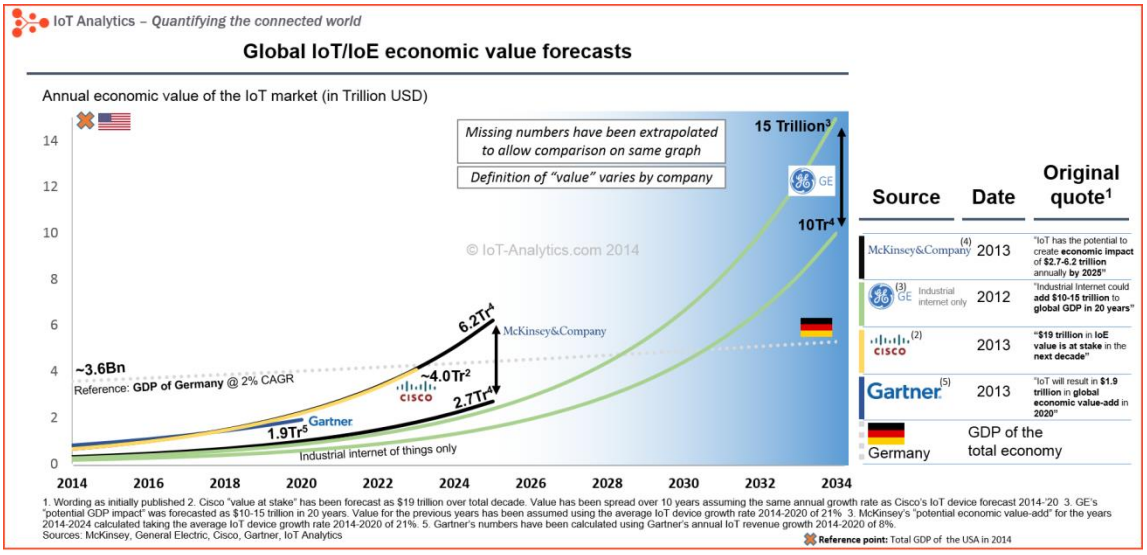
- در حالی که مارکتس‌اندمارکتس درآمد ۱۲۹ میلیاردی را در سال ۲۰۱۴ گزارش می‌کند، IDC قبلاً این رقم را ۲,۳تریلیون دلار گزارش کرده است. در حالی که گارتنر درآمد حدود ۳۰۰ میلیارد دلار در حوزه صنعت را تا سال ۲۰۲۰ پیش‌بینی می‌کند، IDC اعتقاد به رقمی معادل ۷ تریلیون دارد.

به نظر می‌آید عدد گارتنر بسیار محافظه کارانه است. اپل، گوگل و فیس‌بوک با هم تولید درآمد تقریبی ۲۵۰ میلیارد دلاری دارند. اگر گارتنر درست گفته باشد، درآمدکل IoT در حوزه صنعت بعد از ۶ سال فقط کمی بزرگتر از این سه شرکت خواهد بود. با این حال صدها شرکت وجود دارند که در حال حاضر در حال پیوستن به این فناوری هستند. به طور مثال شرکت جنرال الکتریک، با درآمد حدود ۱۵۰ میلیار دلار می‌گوید در حال تغییر سیاست های خود برای پیوستن به IoT است.

از سوی دیگر عدد شرکت IDC بسیار بالا به نظر می‌رسد. ۷ تریلیون دلار در ۶ سال که تقریباً به اندازه نیمی از اقتصاد ایالات متحده است. (۱۶تریلون دلار)

### ۲-۳-۲-۴- مجموع ارزش اقتصادی

سیسکو، GE[۴۶]، گارتنر و مکنزی، پیش‌بینی هایی را برای ارزش IoT برای آینده اقتصاد جهان منتشر کرده‌اند (شکل ۲-۳-۲-۳).




[۴۶] GE

**شکل ۲-۳-۲-۳ پیش‌بینی ارزش جهانی اقتصاد IoT/IoE**

این تجزیه و تحلیل نسبت به سایر موارد مشابه به سه دلیل کمتر آشکار است:

۱- معیار ارزش‌گذاری در پیش‌بینی ها متفاوت است. برای سیسکو معیار "ارزش شرط‌بندی"، برای مکنزی معیار "ارزش اقتصادی"، برای GE معیار "ارزش بالقوه تولید ناخالص جهانی" و برای گارتنر معیار "ارزش افزوده اقتصاد جهانی" است.

۲- گارتنر، GE و مکنزی پیش‌بینی‌هایشان برای تأثیر سالیانه IoT در سال‌های ۲۰۲۰، ۲۰۲۵ و ۲۰۳۴ است.اما سیسکو میزان ۱۹ تریلیون دلار را برای ۱۰ سال آینده پیش‌بینی می‌کند.

۳- هیچ شرکتی نقطه شروع و نرخ رشد ارائه نمی‌دهد. بنابراین نرخ رشد پیش‌بینی شده را می‌توان به عنوان یک پروکسی که مقدار همه سال‌ها از زمان حال تا سال ۲۰۳۴ را شامل می‌شود، در نظر گرفت.

**وجه مشترک پیش‌بینی‌ها:**

- IoT تأثیر عظیم اقتصادی خواهد داشت. اگر پیش‌بینی‌های GE محقق شود، ارزش اینترنت صنعتی در ۲۰ سال، تقریبا به اندازه اقتصاد ایالات متحده امروز خواهد شد.

**اختلاف پیش‌بینی‌ها:**

- وقتی که ارزش اقتصادی وسایل مرتبط یا درآمد صنایع مطرح می‌شود، اختلاف در پیش‌بینی‌ها بسیار کمتر می‌شود. اما بسیار سخت خواهد بود تا تأثیر اقتصادی که دو شرکت مکنزی و GE پیش‌بینی می‌کنند را قبول کرد زیرا یکی رقم بالا و دیگر

## ۲-۴- قلمرو کاربری و حوزه‌های متأثر

[http://iot-analytics.com/10-internet-of-things-applications]

[Haghighi Report]

مجموعه‌ای از اشیاء به هم متصل شده، پتانسیل ارائه خدمات زیادی دارند. مثلا فرض کنید که برنامه کاری خود را وارد تلفن همراهتان کرده‌اید. زمانی که صبح باید از خواب بیدار شوید تا به جلسه برسید، از روی تقویم برنامه کاریتان مشخص می‌شود. نیم ساعت جلوتر از بیدار شدنتان سیستم هوشمند منزل شروع به گرم کردن آب برای

حمام می‌کند. اگر زمستان باشد و حسگرهای منزل تشخیص دهند که دمای هوا در شب به حد یخزدگی رسیده بوده است، برنامهٔ بیدار شدن شما را پنج دقیقه به جلو می‌اندازند تا زمان کافی برای گرم کردن خودرو خود داشته باشید. وضعیت ترافیک توسط خیابان‌های هوشمندِ مجهز به حسگر و خودروهای هوشمند به دست شما می‌رسد. اگر به وسیله نقلیه عمومی نیاز داشته باشید برنامه حرکت آن‌ها به صورت پویا به شما داده می‌شود. برای مثال ممکن است در اثر ترکیدگی لوله آب، یکی از خیابان‌ها موقتا مسدود شده و بنابراین اتوبوس‌های هوشمند، زمان جدید سفر خود و مسیر جایگزین و تأخیر احتمالی را محاسبه و در اختیار اشیاء درخواست کننده این اطلاعات می‌گذارند و برنامه شما برحسب آن ریخته می‌شود تا شما به موقع به جلسه خود برسید.

در مثالی دیگر شبکه برق و لوازم پرمصرف متصل به آن مانند لباسشویی، ظرفشویی و غیره را در منزل در نظر بگیرید. در حال حاضر این اشیاء با یکدیگر ارتباطی ندارند و تنها موجود هوشمند مجموعه، انسان است که آن‌ها را به کار می‌اندازد. اما تصور کنید که انسان تنها دستور کار را به آن‌ها بدهد و هماهنگی و زمان شروع به کار را خود این اشیاء با گفتگو با هم به صورت هوشمندانه تعیین کنند. در این صورت آنها ساعت اوج مصرف شروع به کار نمی‌کنند و درصورتی که اینکار اجتناب ناپذیر باشد، وسایل پرمصرفی مانند لباسشویی و ظرفشویی هم‌زمان با هم دراین بازه شروع به کار نخواهند کرد، چرا که برای شبکه توزیع مضر خواهد بود. این گفتگو میان وسایل برقی می‌تواند از مرزهای یک خانه فراتر رفته و میان وسایل برقی خانه‌های یک محله و یا حتی شهر صورت گیرد تا بار به صورت متعادلی توزیع شود و بالتبع هزینه کمتری برای مشتری نیز به دنبال داشته باشد.

مثال‌هایی که عنوان شد ایده شرکت IBM برای سیاره هوشمند است که بسیار نزدیک به اینترنت اشیاء می‌باشد. توانایی‌های مطرح شده برای IoT، امکان کاربری‌های متعدد را در زمینه‌های مختلف برای آن فراهم می‌کند. بیمارستان‌های هوشمند، سرمایه گذاری‌ها و کارخانه‌های هوشمند در آینده نزدیک وجود خواهند داشت. به طور کلی نیز هدف اینترنت اشیاء، تسهیل و تغییر زندگی بشر به سمت افزایش بهره‌وری و صرفه‌جویی، و کاهش زمان و هزینه‌ها است.

در اینجا به برخی از کاربردهای مهم IoT به صورت موضوعی اشاره می‌کنیم که شامل موارد زیر هستند:

۱- هوا و فضا و صنعت حمل و نقل هوایی

۲- صنعت خودرو

۳- صنعت مخابرات

۴- پزشکی و صنعت بهداشت و درمان

۵- زندگی مستقل

۶- صنعت داروسازی

۷- خرده فروشی و مدیریت زنجیره تامین

۸- صنعت تولید

۹- صنعت نفت و گاز

۱۰- نظارت بر محیط زیست

۱۱- صنعت حمل و نقل

۱۲- زراعت و تولید مثل

۱۳- رسانه و صنعت سرگرمی

۱۴- صنعت بیمه

۱۵- شبکه بازیافت

۱۶- شبکه هوشمند برق

۱۷- معادن و استخراج مواد معدنی

۱۸- خانه هوشمند

۱۹- نظارت بر آزمون‌های سراسری و انتخابات

۲۰- حوزه‌های اجتماعی و شخصی: شبکه‌های اجتماعی هوشمند، یافتن اشیاء گمشده یا دزدیده شده

در ادامه این زیربخش، این کاربردها را با جزئیات بیشتر بررسی می‌نماییم.

### ۲-۴-۱- هوا و فضا و صنعت حمل و نقل هوایی

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

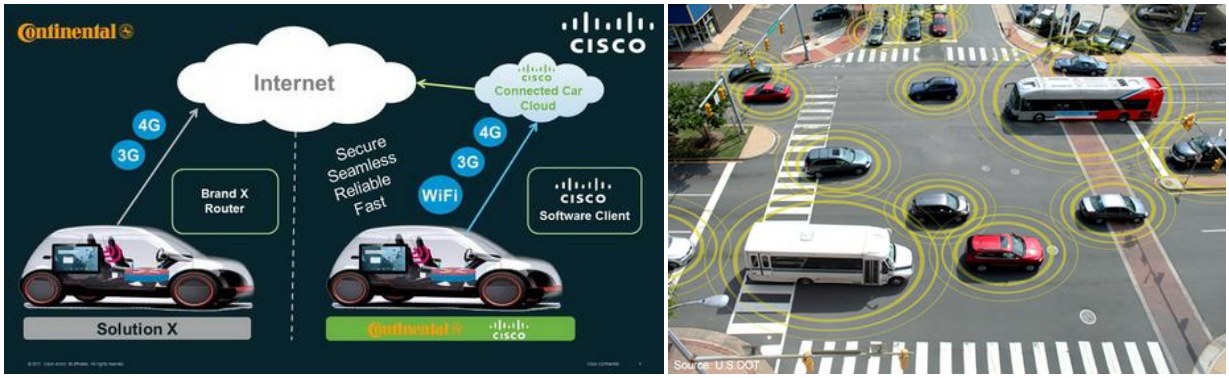
### ۲-۴-۲- صنعت خودرو

ماشین‌های پیشرفته، قطارها، اتوبوس‌ها و حتی دوچرخه‌ها در حال مجهز شدن به حسگرهایی با قدرت پردازش بالا هستند. از جمله کاربردهای IoT در صنعت خودرو می‌توان به کاربرد تجهیزات هوشمند در جهت مشاهده و گزارش پارامترهای متفاوت از فشار داخل تایرها گرفته تا تخمین فاصله از سایر وسایل در حال حرکت درجاده اشاره کرد. تجهیزات متصل شده به قطعات وسایل نقلیه شامل اطلاعاتی همچون نام تولید کننده و زمان و مکان تولید، شماره سریال، نوع کد تولید و نیز محل دقیق آن قطعه در هر وسیله نقلیه هستند. در زمینه صنعت خودرو، تکنولوژی‌هایی همچون (DSRC)[۴۷] ، (V2V)[۴۸] و (V2I)[۴۹] ، سیستم‌های حمل و نقل هوشمندی را ایجاد می‌کنند که نتایج آن ایمنی خودرو و سرنشینان و مدیریت ترافیک است و همگی از زیرساخت‌های IoT محسوب می‌شوند. در شکل ۲-۴-۲-۱ نسل آینده خودرو ها در هنگام ظهور IoT نشان داده شده است.

[۴۷] Dedicated Short Range Communication

[۴۸] Vehicle-to-Vehicle

[۴۹] Vehicle to Infrastructure




شکل ۲-۴-۲-۱ نسل آینده خودروها

## ۲-۴-۳- صنعت مخابرات

IoT قصد دارد فناوری‌های مخابراتی گوناگون را ترکیب کرده و یک سرویس جدید ایجاد کند. به عنوان یک مثال روشن می توان به ترکیب GSM، NFC، Low Power Bluetooth، WLAN، GPS و WSNs با فناوری سیم‌کارت اشاره کرد. در این فناوری قطعه هوشمند بخشی از تلفن همراه خواهد بود و اطلاعات از طریق سیم‌کارت بین سایر وسایل به اشتراک گذاشته می‌شود. فناوری NFC[۵۰] امکان برقراری ارتباطی ساده و امن بین اشیایی که به یکدیگر نزدیک هستند را ایجاد می‌کند (شکل ۲-۴-۳-۱). بنابراین با تلفیق این فناوری و امکانات یک سیم‌کارت می توان توسط یک تلفن همراه مجموعه اشیاء موجود در محل کار و یا منزل را به سادگی برنامه‌ریزی و مدیریت کرد.

[۵۰] Near Field Communication

شکل ۲-۴-۳-۱ ارتباط از طریق تلفن همراه با وسایل اطراف با بهره‌گیری از NFC

### ۲-۴-۴- پزشکی و صنعت بهداشت و درمان

IoT می‌تواند با استفاده از یک تلفن همراه به همراه یک RFID، پارامترهای پزشکی و سلامت و نیز میزان مصرف انواع دارو را کنترل کند. کاشت دستگاه‌های بی‌سیم قابل ردیابی در بدن می‌تواند این امکان را ایجاد کند که علائم حیاتی بدن توسط این دستگاه‌ها در شرایط اضطراری به خصوص برای افراد مبتلا به دیابت، سرطان، بیماری‌های قلبی، سکته مغزی، انسداد ریوی، اختلالات تشنجی و آلزایمر دریافت شود و در مواقع نیاز برای پزشک ارسال شود. همچنین افراد فلج می‌توانند از طریق کاشت سیستم‌های هوشمند محرک عضلانی در بدن خود به بازیابی توان حرکتی قسمت‌های آسیب دیده بدن خود کمک کنند. نظارت از راه دور و به طور مداوم به پزشکان اجازه مراقبت بهتر از بیماران و نیز در صورت لزوم امکان ارائه خدمات پزشکی به آن‌ها را می‌دهد. از جمله کاربردهای IoT در این حوزه می‌توان به لباس هوشمند بچه، تجهیزات نظارت بر سالمندان، بطری‌های هوشمند قرص و دستگاه‌های نظارت بر قلب، خون و سایر قسمت‌های بدن بیماران خاص، را نام برد.

### ۲-۴-۵- زندگی مستقل

IoT و خدمات آن نقش مهمی در ایجاد زندگی مستقل به وسیله حمایت از افراد سالخورده و هدایت فعالیت‌های روزانه آن‌ها دارد. با استفاده از پوشیدنی‌های مجهز به حسگرها، می‌توان بر تعاملات اجتماعی آن‌ها نظارت داشت و یا حتی بیماری‌های مزمن و علائم حیاتی آن‌ها را مشاهده کرد و به طور کلی همه نظارت‌های ذکر شده در بخش ۱-۴-۱ را از راه دور بر آن‌ها داشت و در صورت نیاز به کمک آن‌ها شتافت.

### ۲-۴-۶- صنعت داروسازی

برای محصولات دارویی، امنیت و ایمنی بیشترین اهمیت را دارد. در IoT با اتصال برچسب‌های هوشمند به مواد دارویی به راحتی می‌توان زنجیره تولید و عرضه آن‌ها را کنترل و نظارت کرد. به عنوان مثال، اقلامی که نیاز به

ذخیره‌سازی در شرایط خاص دارند (مانند داروهایی که حتما باید در دمای خاصی نگهداری شوند) را می توان به طور مداوم نظارت کرد و در صورتی که این شرایط در طول حمل و نقل دارو نقض شود از ورود آن‌ها به بازار خودداری نمود. از همه مهم‌تر آن که، به واسطه این فناوری می‌توان مواد دارویی جعلی را تشخیص داد. همچنین برچسب‌های هوشمند قادرند تا از طریق اعلام دستورالعمل‌های لازم جهت نگهداری، نحوه استفاده و تاریخ انقضای دارو به بیمار کمک بسیاری کنند.

### ۲-۴-۷- خرده فروشی و مدیریت زنجیره تامین

IoT می‌تواند چندین مزیت در خرده فروشی و مدیریت زنجیره تامین ارائه دهد. به عنوان مثال با مجهز کردن قفسه‌های کالا به تجهیزاتی همچون RFIDها، یک خرده فروش می‌تواند نیازمندی‌های کالاهای خود را به درستی مدیریت کند. همچنین اگر تولید کنندگان عمده، اطلاع از میزان نیاز خرده‌فروشان داشته باشند بهتر می‌توانند تولیدات خود را مدیریت کرده و وضعیت بازار را کنترل کنند. بنابراین با جمع‌آوری اطلاعات ارسال شده از نیازمندی‌های خرده‌فروشان، می‌توانند تولیدات خود را بهینه کنند. IoT می‌تواند یک پتانسیل عظیم جهت انبارسازی محصولات در خرده فروشی‌ها ایجاد کند. طبق آمار سالیانه حدود ۳,۹ درصد از فروش خرده‌فروشان به دلیل کمبود کالا از بین می‌رود. بنابراین این فناوری با نمایش لحظه‌ای میزان موجودی و فروش هر کالا قادر است نقش بزرگی در زنجیره تولید و عرضه کالاها ایفا کند (شکل ۲-۴-۷-۱).

شکل ۲-۴-۷-۱ کاربرد اینترنت اشیاء در مدیریت اقلام داخلی فروشگاه

### ۲-۴-۸- صنعت تولید

به واسطه ارتباط اشیاء با فناوری اطلاعات و نیز حمایت از زیرساخت‌های شبکه و سیستم‌های اطلاعاتی می‌توان فرآیند تولید هر محصول را بهینه‌سازی کرد و کل چرخه عمر اشیاء را از تولید تا زمانی که به دست مصرف‌کننده می‌رسند نظارت کرد. تجهیزات IoT امکانات بسیاری به منظور نظارت بدون وقفه، از شرایط تولید محصولات در کارخانه ها و عرضه آن‌ها به بازارهای فروش در اختیار مسئولین قرار می‌دهد.

### ۲-۴-۹- صنعت نفت و گاز

با استفاده از زیرساخت‌های IoT و ادغام نظارت‌های بی‌سیم می‌توان بر نظارت پرسنل در شرایط حساس عملیات خشکی و دریایی، ردیابی کانتینرها، ردیابی قطعات مته و رشته های لوله، نظارت و مدیریت تجهیزات ثابت تسلط کامل داشت. با بررسی حوادث در بخش شیمیایی و پتروشیمی انگلستان، آشکار شد که برخی از مشخصه‌های این حوادث مانند عدم وجود مدیریت و کنترل ضعیف بر ذخیره سازی، پردازش و فرآیند جدایی شیمیایی، مشترک بودند. IoT می‌تواند با تجهیز ظروف و مواد شیمیایی خطرناک به حسگرهای بی‌سیم نقش بزرگی در کاهش حوادث نفت و گاز داشته باشد.

### ۲-۴-۱۰- نظارت بر محیط زیست

استفاده از ابزارهای قابل شناسایی بی‌سیم در محیط زیست از دیگر مزایای IoT است که امکان نظارت تمام وقت محیط زیست و کنترل تغییرات انواع گونه‌های حیوانی و گیاهی را برای ما فراهم می‌کند. با استفاده از حسگرهایی که در سطح جنگل‌ها توزیع شده‌اند می‌توان از آتش‌سوزی‌های وسیع که سالانه در جنگل‌های جهان اتفاق می‌افتد، جلوگیری کرد. همچنین با بهره‌گیری از شبکه حسگرهای بی‌سیم که در سطح شهر پخش شده‌اند می‌توان به طور لحظه‌ای از میزان آلاینده‌های موجود در هوا، در نقاط مختلف شهر اطلاع دقیق پیدا کرد. دستگاه‌های مجهز به حسگرهای متفاوت، از نزدیک مدام محیط زیست را نظارت می‌کنند و اطلاعات بسیاری از قبیل تغییرات در ساختار شهرها، جمع آوری اطلاعات در مورد فاضلاب‌ها، کیفیت هوا و دفع زباله‌ها را در اختیار ما قرار می‌دهند. مشاهده و

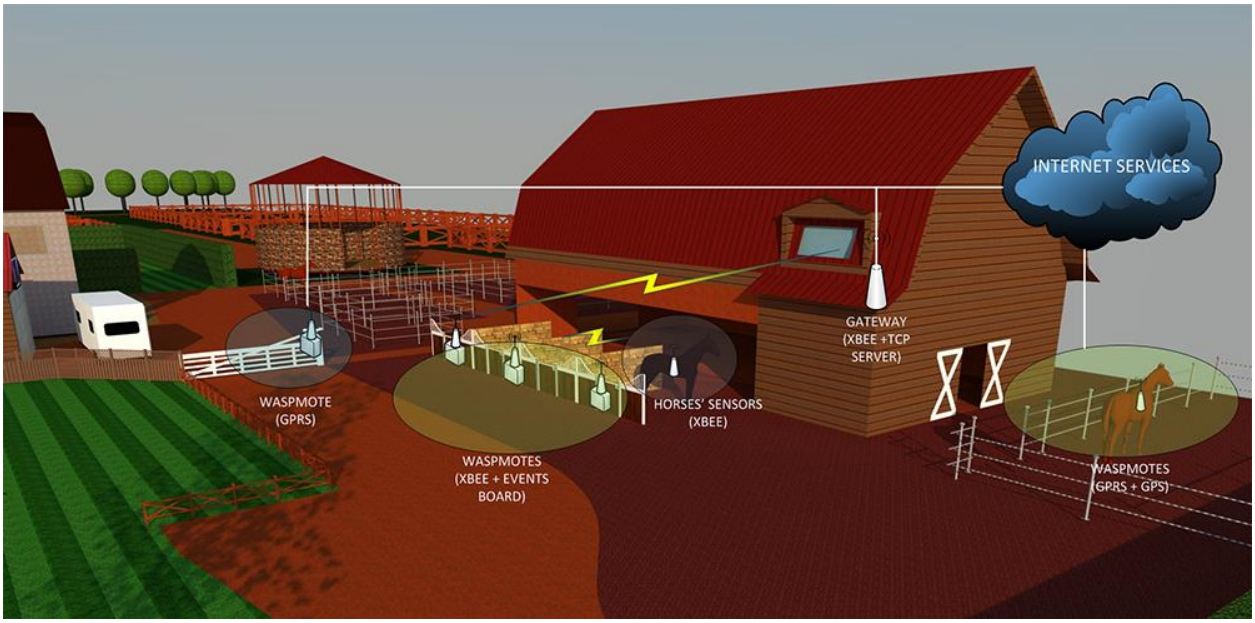
اندازه‌گیری بسیاری از تغییرات زیست محیطی بسیار دشوار است و در واقع IoT با در اختیار قرار دادن اطلاعات جمع‌آوری شده در مورد این مشاهدات اولین قدم برای درک اثرات عوامل انسانی و غیر انسانی در ایجاد دگرگونی در محیط زیست برای ما فراهم می‌کند. از جمله مهم‌ترین کاربردهای IoT در این حوزه می‌توان به دستگاه‌های هوشمند کنترل لحظه‌ای هوای اطراف، سطل زباله‌های هوشمند و دستگاه‌های هوشمند مسیریابی دریایی اشاره کرد.

### ۲-۴-۱۱- صنعت حمل و نقل

IoT روش‌های بسیاری برای جمع‌آوری کرایه و یا پرداخت عوارض ارائه می‌دهد. همچنین این فناوری به امنیت انتقال بار و جابجایی مسافران بسیار کمک می‌کند. با استفاده از تجهیزات این فناوری می‌توان عملیات ردیابی بار و مسافر را به راحتی در شبکه خطوط حمل‌ونقل به‌ویژه خطوط هوایی انجام داد. از همه جالب‌تر آن که با اعلام وضعیت ترافیک راه از طریق تلفن همراه به مسافران، شرایط حمل و نقل کالا و مسافر را بسیار بهینه می‌کند.

### ۲-۴-۱۲- زراعت و تولید مثل

قابلیت ردیابی حیوانات اهلی و مدیریت میزان یارانه‌ای که به نسبت تعداد حیوانات گله‌داران، به آن‌ها تعلق می‌گیرد، بدون وجود تقلب، امکان دیگری است که IoT برای ما محیا می‌کند. با نصب سیستم‌های شناسایی دام و طیور می‌توان از وضعیت واکسینه شدن آن‌ها و یا از شیوع انواع بیماری‌ها در میان آن‌ها پیشگیری کرد و یا حتی وضعیت ریشه‌کن شدن یک بیماری را در بین حیوانات بررسی کرد و یا حتی اطلاعات دقیق از تعداد حیوانات و میزان تولیدات دامی و کشاورزی در طول دوره‌های زمانی از یک کشور معین و یا تمام دنیا به دست آورد (شکل ۲-۴-۱۲-۱).




شکل ۲-۴-۱۲-۱مدیریت اصطبل پرورش اسب با حسگرهای نصب شده در آن

### ۲-۴-۱۳- رسانه و صنعت سرگرمی

گسترش IoT این امکان را فراهم می‌آورد تا اخبار مورد نیاز هر کاربر براساس محلی که او در آن قرار دارد توزیع شود. همچنین می‌توان با توجه به این که مردم در هر منطقه‌ای که زندگی می‌کنند اخبار و اطلاعات خود را توسط کدام یک از رسانه‌های جمعی به دست می‌آورند، اخبار را میان آن‌ها به اشتراک گذاشت. علاوه‌براین برچسب‌های ارتباط نزدیک را می‌توان بر روی پوسترها، جهت ارائه اطلاعات بیشتر نصب کرد.

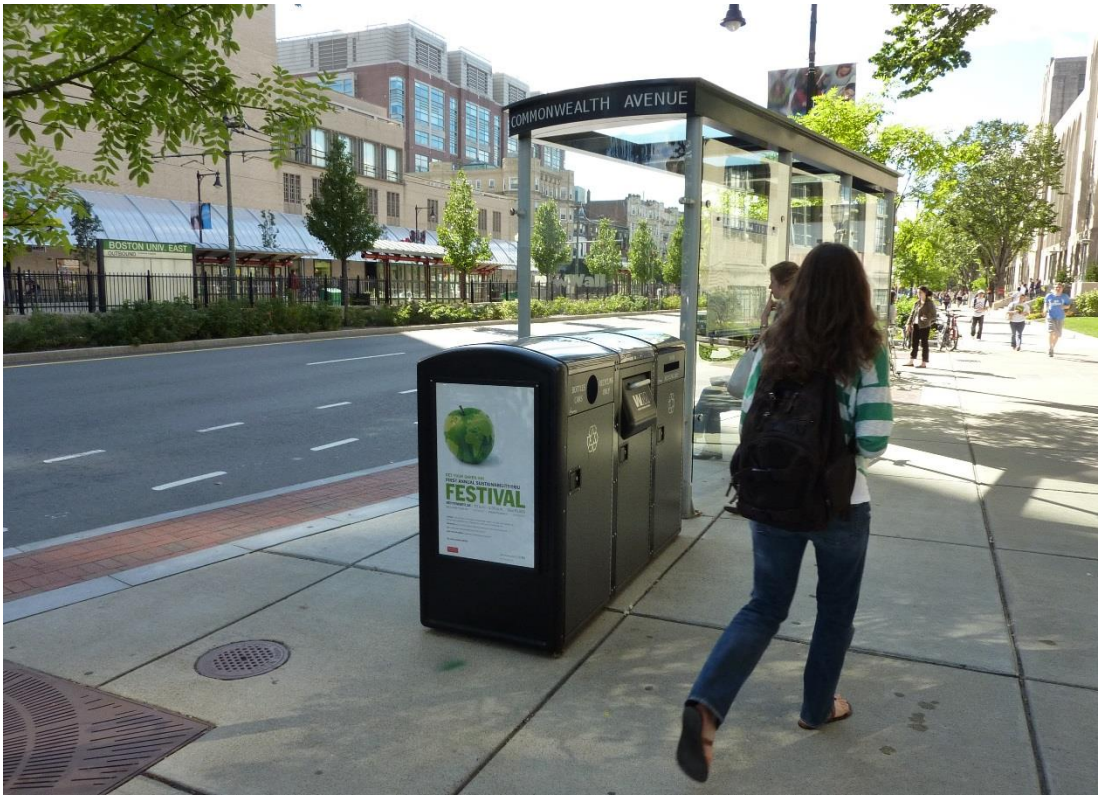
### ۲-۴-۱۴- صنعت بیمه

فرض کنید که خودرو شما قادر به ثبت خودکار شتاب، سرعت و دیگر پارامترها باشد. شرکت بیمه به هنگام بروز تصادف با دریافت اطلاعات، قادر به پرداخت بهینه حق بیمه در مدت زمان کمتری خواهد بود. حال شرکت‌های بیمه می‌توانند بخشی از پس‌انداز ناشی از این اقدام را به عنوان تخفیف به مشتریان خود بدهند. همین امر برای دارایی‌های دیگر همچون خانه، ماشین آلات و غیره قابل تعمیم است. البته این امر نیازمند آن است که افراد قبول کنند تا

اطلاعات خصوصی آن‌ها در اختیار دیگران قرار بگیرد. در واقع بعضی وقت‌ها مردم به ازای دریافت خدمات بهتر و یا منعفت مالی بیشتر حاضر به قبول این موضوع هستند.

### ۲-۴-۱۵- شبکه بازیافت

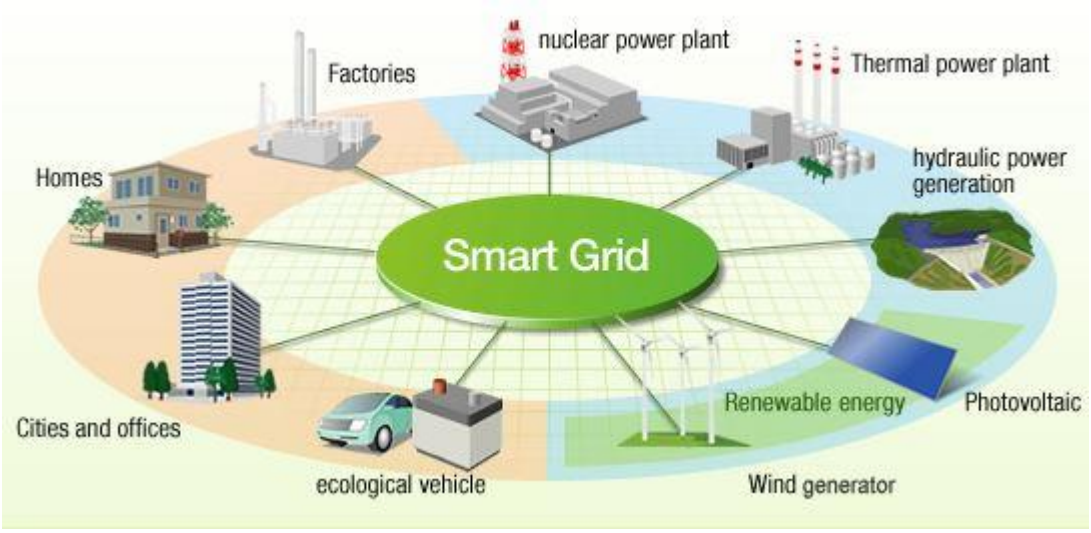
از IoT می توان برای کنترل انتشار وسایل نقلیه جهت نظارت و کنترل بر آلودگی هوا، دسته بندی و غربال انواع زباله و استفاده مجدد از قطعات الکترونیکی و دفع انواع زباله استفاده کرد. در واقع این تجهیزات RFID هستند که با ارائه اطلاعات از انواع وسایل، کار شناختن و جداسازی زباله‌ها را برای ما میسر می‌سازند. همچنین این تجهیزات به کاهش زباله‌ها به خصوص زباله‌های الکترونیکی و نیز جلوگیری از انتشار زباله‌های خطرناک در محیط زیست کمک می‌کنند (شکل ۲-۴-۱۵-۱). تجهیزات RFID با برآورد نیازهای کاربران باعث کاهش حمل و نقل و در نتیجه کاهش میزان آلودگی می‌شوند به صرفه‌جویی در وقت و هزینه بسیار کمک می‌کنند.



شکل ۲-۴-۱۵-۱ سطل زباله‌های هوشمند

### ۲-۴-۱۶- شبکه هوشمند برق

شبکه‌های هوشمند یک مورد خاص هستند. این شبکه‌ها در آینده با استفاده مکانیزه از اطلاعات تأمین‌کنندگان و مصرف‌کنندگان برق، به بهبود کارایی و قابلیت اطمینان اقتصادی در صنعت برق کمک می‌کنند. ۴۱۰۰۰ جست‌وجوی ماهانه در گوگل، برجسته بودن این موضوع را نشان می‌دهد. حسگرها برای سیستم‌های شبکه هوشمند ضروری هستند چرا که به اپراتورها این امکان را می‌دهند تا میزان استفاده و عملکرد شبکه را در هر لحظه اندازه بگیرند. این بدین معنی است که به جای این‌که منتظر تماس مشتریانی شوند که برق آن‌ها قطع شده است، شرکت‌های تولید برق می‌توانند نقطه قطع برق را تشخیص داده و با تغییر مسیر انتقال توان و یا تولید تجهیزات جدید، جریان برق را به نقطه قطع شدگی هدایت کنند.مدیریت این حسگرها از کاربردهای اساسی و مهم اینترنت اشیاء می‌باشد. کنتورهای هوشمند و دارای قابلیت ارتباط دوطرفه می‌توانند زمان قطع انرژی را کاهش داده و تشخیص علت قطع شدگی را سریع‌تر کنند (شکل ۲-۴-۱۶-۱).



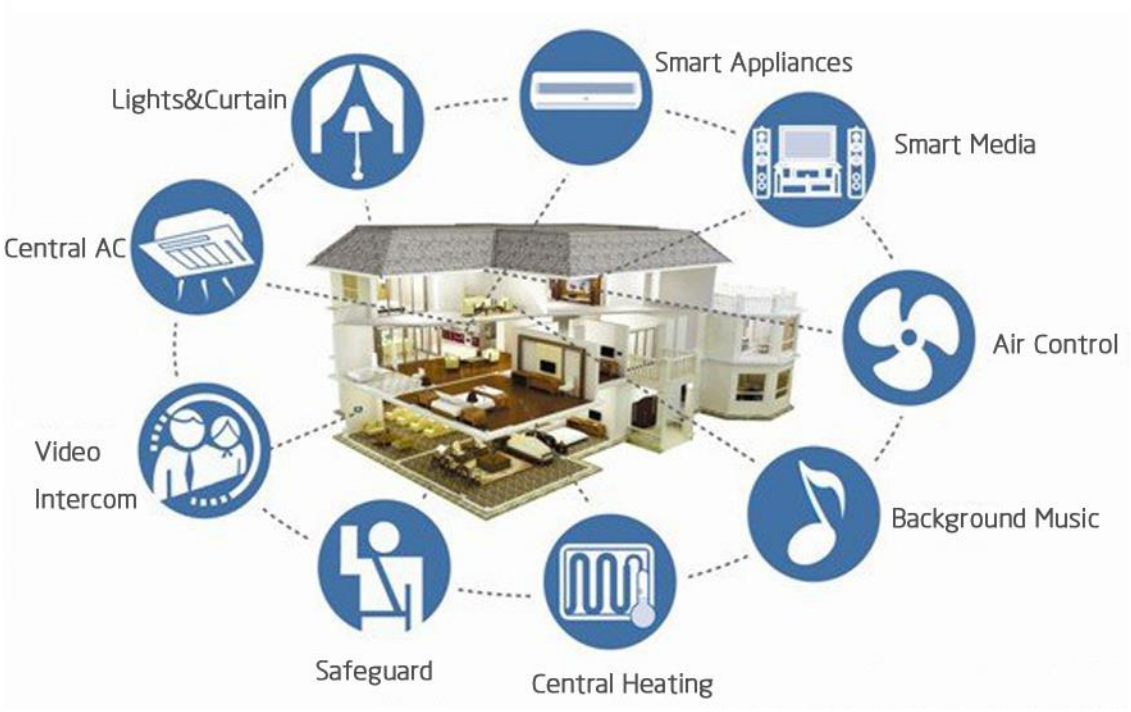

شکل ۲-۴-۱۶-۱ شبکه‌های هوشمند برق به کاهش هزینه‌های برق کمک می‌کنند

### ۲-۴-۱۷- معادن و استخراج مواد معدنی

در صنایع نفت، فلز و استخراج مواد معدنی، فناوری اینترنت اشیاء می‌تواند در پیدا کردن ذخایر معدنی و افزایش قابلیت بازیافت مؤثر باشد. اطلاع لحظه‌ای از میزان استخراج مواد معدنی از ذخایر مختلف و مدیریت آن‌ها از راه دور قابلیتی است که اینترنت اشیاء در اختیار ما قرار می‌دهد.

### ۲-۴-۱۸- خانه هوشمند

در یک خانه هوشمند وسایل الکتریکی درون خانه به یکدیگر متصل‌اند و از طریق اینترنت اشیاء قابلیت مدیریت آن‌ها توسط ما کارآمدتر خواهد بود. تصور کنید که برای مسافرت از خانه خارج شده‌اید و فراموش کرده باشید که چراغ‌های منزل را خاموش کنید و یا کنتور گاز و آب را قطع کنید. این‌لحظه همان موقعی است که اینترنت اشیاء به کمک شما می‌آید و به شما این امکان را می‌دهد تا از دور نیز بر وسایل و ابزارهای درون منزلتان مدیریت داشته باشید. و یا حتی در مواقعی که در منزل نیستید و قرار است سرقتی از منزلتان رخ دهد به صورت لحظه‌ای باخبر شده و پلیس را در جریان بگذارید (شکل ۲-۴-۱۸-۱).



شکل ۲-۴-۱۸-۱ خانه هوشمند

## ۲-۴-۱۹- نظارت بر آزمون‌های سراسری و انتخابات

یکی از موضوعاتی که در کشورمان مطرح است، بحث اجرای آزمون‌های سراسری توسط سازمان سنجش می‌باشد. این سازمان همه ساله با چالش محرمانه ماندن سوالات تا قبل از اجرای آزمون روبرو است. با استفاده از اینترنت اشیاء و قرار دادن تگ‌های RFID در بسته‌های حاوی سوالات می‌توان از موقعیت و پلمپ ماندن این بسته‌ها تا قبل از اجرای آزمون اطمینان حاصل کرد. در بحث انتخابات نیز میزان آراء در هر منطقه و موقعیت مکانی صندوق‌های رأی‌گیری در هر لحظه را با زدن برچسب های RFID بر صندوق‌ها و سربرگ‌های رأی از طریق اینترنت اشیاء و از راه دور کنترل کرد.

حال که برخی از کاربردهای اساسی اینترنت اشیاء ذکر شد در زیر بخش بعدی به رتبه بندی این کاربردها از نظر اهمیت در زندگی روزمره افراد، که توسط مؤسسه IoT آنالیتیک[۵۱] انجام شده می‌پردازیم.

## ۲-۴-۲۰- ده عدد از محبوب‌ترین کاربردهای حال حاضر اینترنت اشیاء

[http://iot-analytics.com/10-internet-of-things-applications]

نیازی به گفتن نیست که اعتیاد به IoT بسیار گسترده می‌باشد. هر روز یک شرکت جدید برخی از محصولات IoT خود را اعلام می‌کند. مؤسسه IoT آنالیتیک بنا بر رسالت خود و با توجه به داده‌های موجود در بستر اینترنت، به رتبه بندی کاربردهای اینترنت اشیاء از نظر اهمیت آن‌ها برای افراد، اقدام کرده است. در این رتبه‌بندی خانه‌های هوشمند به عنوان برجسته‌ترین برنامه IoT قرار می‌گیرند (شکل ۲-۴-۲۰-۱).

نحوه رتبه بندی توسط این مؤسسه به این نحو است که سه معیار مد نظر قرار می‌گیرد:

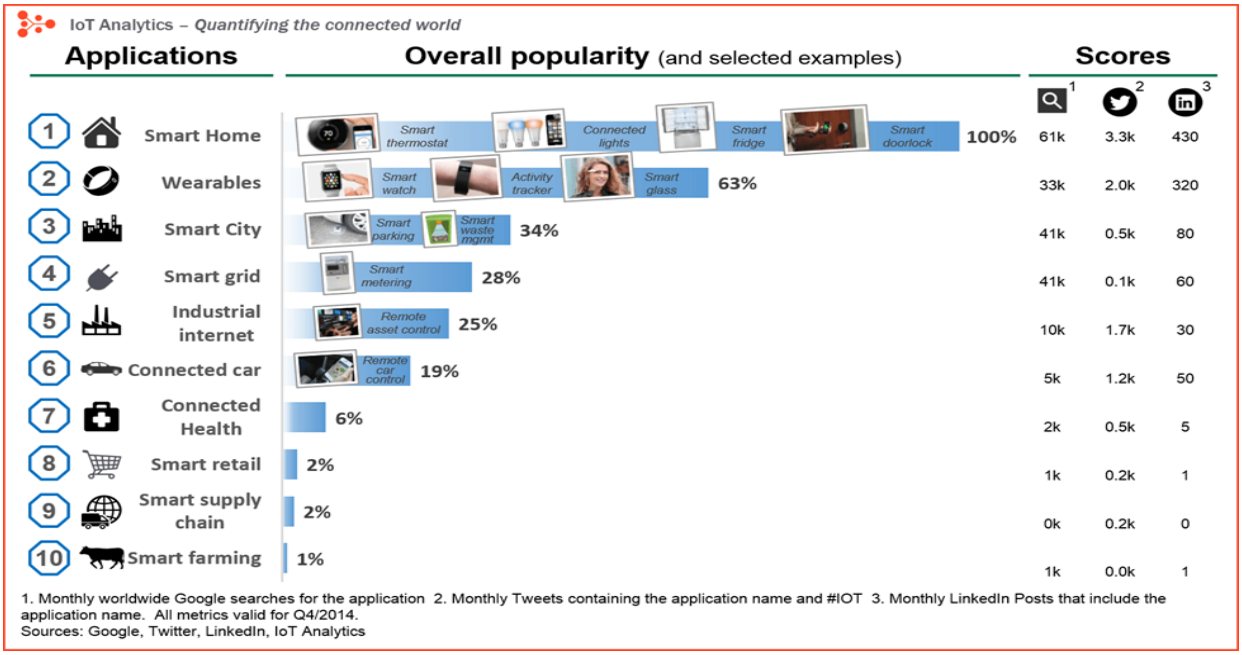
۱- آنچه مردم در گوگل جست‌وجو می‌کنند

۲- ۲- آنچه مردم در توییتر راجع به آن صحبت می‌کنند

[۵۱] Iot-analytics

۳- ۳- آنچه مردم در لینکدین[۵۲] درباره آن می‌نویسند.

بالاترین امتیاز رتبه ۱۰۰ درصد را دریافت می‌کند و سایر کاربردها نسبت به آن سنجیده می‌شوند.




**شکل ۲-۴-۲۰-۱ رتبه بندی کاربردهای اینترنت اشیاء**

در ادامه به بررسی این ۱۰ کاربرد از دیدگاه مؤسسه IoT آنالیتیک می‌پردازیم.

### ۲-۴-۲۰-۲- خانه هوشمند

خانه هوشمند به عنوان بالاترین کاربرد IoT در تمامی معیارهای اندازه‌گیری است. بیش از ۶۰۰۰۰ نفر در هر ماه اصطلاح "خانه هوشمند" را جست‌وجو می‌کنند. پایگاه داده مؤسسه IoT آنالیتیک شامل ۲۵۶ مؤسسه و شرکت دانش‌بنیان می‌باشد. این شرکت‌ها بیشتر در زمینه خانه هوشمند فعالیت می‌کنند ، تعداد کل شرکت‌های دانش‌بنیانی که روی موضوع خانه هوشمند کار می‌کنند در حال حاضر بیش از ۲,۵میلیارد است. این لیست شامل اسامی

[۵۲] Linkedin

شرکت‌های برجسته‌ای مانند نست[۵۳] و آلرت‌می[۵۴] همچنین شرکت‌های چند ملیتی مانند فیلیپس[۵۵]، هایر[۵۶] و یا بلکین[۵۷] است.

### ۲-۴-۲۰-۳- پوشیدنی‌ها

بحث پوشیدنی‌ها یک بحث بسیار داغ است. مصرف‌کنندگان منتظر ساعت هوشمند جدید شرکت اپل در ماه آپریل سال ۲۰۱۵ هستند. نوآوری‌های هیجان‌انگیز دیگری نیز وجود دارند که از آن‌جمله می‌توان سیستم کنترل حرکت میو[۵۸] و یا دستبند لوک‌سی[۵۹] را نام برد. در میان همه مراکز IoT، فروشگاه پوشیدنی‌های جابن[۶۰] احتمالاً یکی از بزرگترین آن‌ها است. این فروشگاه بیش از نیم میلیارد دلار فروش دارد.

### ۲-۴-۲۰-۴- شهر هوشمند

شهرهای هوشمند طیف کاربری گسترده‌ای، از مدیریت ترافیک گرفته تا توزیع آب، مدیریت ضایعات، امنیت شهری و نظارت بر محیط زیست را دارند. محبوبیت این کاربرد به خاطر این واقعیت است که بسیاری از مشکلات شهری را به وسیله آن می‌توان حل کرد. با استفاده از IoT برای شهرهای هوشمند می‌توان ازدحام ترافیک و سروصدا و آلودگی را کم کرد و به ایجاد شهرهای امن تر کمک نمود.

---

[۵۳] Nest

[۵۴] Alertme

[۵۵] Philips

[۵۶] Haier

[۵۷] Belkin

[۵۸] Myo

[۵۹] Looksee

[۶۰] Jowbone

### ۲-۴-۲۰-۵- شبکه‌های هوشمند

شبکه‌های هوشمند یک مورد خاص هستند. این شبکه‌ها در آینده با استفاده مکانیزه از اطلاعات تأمین‌کنندگان و مصرف‌کنندگان برق، به بهبود کارایی و قابلیت اطمینان اقتصادی در صنعت برق کمک می‌کنند. همچنین، ۴۱۰۰۰ جست‌وجوی ماهانه در گوگل، برجسته بودن این موضوع را نشان می‌دهد.

### ۲-۴-۲۰-۶- اینترنت صنعتی

اینترنت صنعتی نیز یکی از کاربردهای اینترنت اشیاء است. در حالی که بسیاری از محققان بازار مانند گارتنر[۶۱] یا سیسکو[۶۲] مفهوم اینترنت صنعتی را به عنوان مفهومی از IoT با بیشترین پتانسیل کاربری می‌بینند. اما محبوبیت آن در حال حاضر به خانه هوشمند و پوشیدنی‌ها نمی‌رسد. از این مفهوم به نسبت سایر مفاهیم بسیار کمتر در توییتر صحبت می‌شود.

### ۲-۴-۲۰-۷- ماشین متصل[۶۳]

ماشین متصل به آرامی خواهد آمد. علی‌رغم این‌که پیشرفت در صنعت خودرو به طور معمول ۲ تا ۴ سال طول می‌کشد، اما هنوز شاهد تغییرات در صنعت ماشین متصل نبوده‌ایم. اکثر خودروسازان بزرگ و همچنین برخی از مؤسسات، در حال کار بر روی راه‌حل‌های ماشین متصل هستند. اگر شرکت‌های بزرگ خودروسازی مانند بی‌ام‌و[۶۴] و فورد[۶۵] به زودی نسل بعدی ماشین متصل را ارائه نکنند، دیگر غول‌های شناخته شده همچون گوگل، مایکروسافت، و اپل همگی پلتفرم‌های ماشین متصل را ارائه خواهند داد.

---

[۶۱] Gartner

[۶۲] Cisco

[۶۳] Connected car

[۶۴] BMW

[۶۵] Ford

### ۲-۴-۲۰-۸- سلامت متصل[۶۶]

سلامت متصل در حوزه IoT یک بازار خاموش است، چرا که تا کنون توجهی به آن نشده است. علی‌رغم این بی‌توجهی، اما در آینده نزدیک، یکی از حوزه‌های تأثیرگذاری IoT خواهد بود که هم به درآمدزایی شرکت‌ها و هم به رفاه مردم کمک خواهد کرد.

### ۲-۴-۲۰-۹- خرده‌فروشی هوشمند

خرده‌فروشی هوشمند، به معنی تسهیل و هوشمندسازی خرده‌فروشی است. البته این بخش از کاربردهای IoT در مقایسه با بخش‌های گفته شده در بالا از محبوبیت کمتری برخوردار هستند. به عنوان مثل، این امر را می‌توان با بررسی سایت لینکدین تأیید کرد که برای خرده‌فروشی هوشمند تنها یک پست در ماه ثبت شده است، حال آنکه خانه هوشمند ۴۳۰ پست در ماه را به خود اختصاص داده است.

### ۲-۴-۲۰-۱۰- زنجیره تأمین هوشمند

زنجیره تامین چند سالی است که هوشمند شده است. ردیابی کالاها در حالی که آن‌ها در جاده‌ها هستند، یا به دست آوردن لیست موجودی بازار برای تأمین کنندگان کالا از راه‌حل‌های این فناوری است. بنابراین کاملاً منطقی است که این عنوان در حوزه IoT قرار بگیرد.

### ۲-۴-۲۰-۱۱- کشاورزی هوشمند

کشاورزی هوشمند اغلب در IoT نادیده گرفته می‌شود. چرا که به دسته‌های شناخته‌شده مانند بهداشت، حمل‌ونقل و یا صنعتی تعلق ندارد. با این حال، با توجه به وسعت و دوری زمین‌های کشاورزی و تعداد زیاد دام امکان نظارتی که IoT ایجاد می‌کند، می‌تواند انقلابی در کشاورزی ایجاد کند. اما این ایده هنوز در مقیاس بزرگ مورد توجه قرار ندارد. با این حال یکی از کاربردهای IoT است که نباید دست کم گرفته شود. کشاورزی هوشمند همچنین می‌تواند به صادرات محصولات کشاورزی نیز کمک کند.

---

[۶۶] Connected Health

در خاتمه این زیر بخش به پروتکل‌های مورد نیاز IoT برای ایجاد ارتباط متصل در حوزه‌های کاربری آن اشاره می‌کنیم. اینترنت اشیاء قصد محیا کردن زیرساخت‌هایی جهت برقراری ارتباط بین اشیاء و نیز ارتباط اشیاء با محیط پیرامون خود دارد. این فناوری زودی انقلاب بزرگی در تمامی جنبه‌های زندگی بشر ایجاد خواهد کرد. هدف این فناوری وارد شدن به تمام حوزه‌های زندگی بشر به منظور ساده‌تر کردن آن و ایجاد کارایی بیشتر در ابزارهایی است که انسان جهت رفع نیازهای خود مورد استفاده قرار می‌دهد. اما آنچه که مشخص است آن است که با ارتباط اشیاء با هم حجم وسیعی از داده‌ها در هر لحظه و در هر مکان جریان خواهد داشت. پس مدیریت این جریان داده و به کارگیری آن به منظور مصارف مهمی همچون اقتصادی و اجتماعی بسیار چالش برانگیز خواهد بود. شکل ۲-۴-۲۰-۱ پروتکل‌های مورد نیاز در هر بخش را بیان می‌کند.


**شکل ۲-۴-۲۰-۱برخی از کاربردهای IoT در حوزه‌های مختلف و پروتکل‌های مورد نیاز آن‌ها**

## ۲-۵- بررسی اینترنت اشیاء از دیدگاه مؤسسه جهانی مکنزی

[MGI_Disruptive_technologies_Full_report_May2013]

مؤسسه جهانی مکنزی[۶۷] (MGI)، بازوی تحقیقاتی تجارت و اقتصاد شرکت مکنزی است که در سال ۱۹۹۰ به منظور درک عمیق‌تر تحول اقتصادی جهان تأسیس شد. هدف این مؤسسه فراهم کردن رهبرانی در بخش‌های تجاری، عمومی و اجتماعی با علم و بصیرت بر مدیریت پایه‌ای[۶۸] و تصمیمات سیاسی است.

MGI رشته‌های اقتصاد و مدیریت را با هم ترکیب می‌کند و ابزارهای تحلیل اقتصاد را به همراه بینش و بصیرت رهبران تجاری به خدمت می‌گیرد. روش این مؤسسه موسوم به "micro-to-macro" گرایش اقتصاد خرد را برای درک بهتر توانایی‌های گسترده اقتصاد کلان مورد بررسی قرار می‌دهد که بسیار بر استراتژی تجارت و سیاست‌های عمومی تأثیر گذار است. گزارش‌های MGI بیش از ۲۰ کشور و ۳۰ صنعت را تحت پوشش قرار می‌دهد. پژوهش حاضر بر چهار موضوع بهره‌وری[۶۹] و رشد، تکامل بازارهای مالی جهانی، تأثیر اقتصادی فناوری و نوآوری، و شهری‌سازی[۷۰] تمرکز دارد. گزارش‌های اخیر، ایجاد شغل، بهره‌وری منابع، شهرهای آینده و تأثیر اینترنت را بررسی کرده‌اند.

مؤسسه MGI توسط Ricahrd Dobbs و James Manyka هدایت می‌شود. تیم‌های پروژه توسط یک گروه از افراد ارشد هدایت می‌شوند و شامل مشاوران متعدد از دفاتر مؤسسه MGI از سراسر جهان هستند. این تیم‌ها، شرکا و حرفه‌ای‌های مدیریت و صنعت را در شبکه جهانی مکنزی گرد هم می‌آورند. علاوه بر این رهبران اقتصادی شامل (برندگان جایزه نوبل) نیز به عنوان مشاوران پروژه عمل می‌کنند.

### ۲-۵-۱- نرخ ارتباط توسعه و دستاوردها

نرخ ارتباط توسعه و دستاوردها از دیدگاه مؤسسه مکنزی به صورت موضوعی در ذیل آمده است.

- ۵ میلیون دلار در مقابل ۴۰۰ دلار: قیمت ابرکامپیوتر در سال ۱۹۷۵ در مقابل آیفون ۴ با عملکرد برابر

---

[۶۷] Mckinsey

[۶۸] Base management

[۶۹] Productivity

[۷۰] Urbanization

- بیش از ۲۳۰ میلیون پژوهشگر[۷۱] در سال ۲۰۱۲
- ۲,۷ میلیارد دلار، ۱۳سال: قیمت و هزینه پروژه Human Genome که در سال ۲۰۰۳ به اتمام رسید.
- بیش از ۳۰۰۰۰۰ مایل رانده شده توسط اتومبیل‌های بدون سرنشین گوگل تنها با یک تصادف (به دلیل خطای انسانی)
- 3x. افزایش در کارایی چاه‌های گاز در آمریکای شمالی در سال‌های ۲۰۰۷ تا ۲۰۱۱
- ۸۵ درصد، کاهش در هزینه برای هر وات از یک سلول فتوولتائیک[۷۲] از سال ۲۰۰۰ تا کنون

### ۲-۵-۲- پتانسیل‌های اقتصادی در سال ۲۰۲۵

پتانسیل‌های اقتصادی در سال ۲۰۲۵ از دیدگاه مؤسسه مکنزی به صورت موضوعی در ذیل آمده است.

- ۲-۳ میلیارد مردم بیشتر برای دسترسی به اینترنت در سال ۲۰۲۵.
- ۵-۷ تریلیون دلار: تأثیر اقتصادی اتوماسیون کار دانش[۷۳] تا سال ۲۰۲۵.
- ۱۰۰دلار و یک ساعت: هزینه و زمان یک ژن انسانی[۷۴] در یک دهه آینده.
- ۱,۵میلون مرگ و میر ناشی از تصادف راننده‌ها در سال ۲۰۲۵ که به طور بالقوه توسط وسایل نقلیه خودکار قابل کاهش هستند.
- ۱۰۰-۲۰۰ درصد افزایش بالقوه در تولید روغن آمریکای شمالی تا سال ۲۰۲۵.
- ۱۶درصد سهم بالقوه از تولید برق با انرژی خورشیدی و بادی تا سال ۲۰۲۵.

---

[۷۱] Knowledge worker

[۷۲] Photovoltaic

[۷۳] Knowledge work

[۷۴] Human Genome

## ۲-۵-۳- اینترنت اشیاء از دیدگاه مؤسسه مکنزی

اشیاء فیزیکی به طور فزاینده در دنیای متصل[۷۵] در حال افزایش هستند. ماشین آلات، محموله‌ها، زیرساخت‌ها و دستگاه‌ها همگی به شبکه‌ای از حسگرها و محرک‌ها مجهز شده‌اند که امکان نظارت بر محیط خود، گزارش وضعیت، دریافت دستورالعمل و حتی اقدام بر اساس اطلاعاتی که دریافت می‌کنند را فراهم می‌کند. حتی به عنوان مثال افراد می‌توانند با حسگرهای فعال مجهز شوند تا بتوانند وضعیت سلامت خود را پیگیری کنند. این چیزی است که به اصطلاح "اینترنت اشیاء" نامیده شده است و به سرعت در حال رشد است. بیش از ۹ میلیارد دستگاه در سراسر جهان از جمله کامپیوترها و گوشی‌های هوشمند در حال حاضر به اینترنت متصل هستند و انتظار می‌رود که این تعداد تا دهه آینده افزایش چشمگیری پیدا کند و به حدود یک تریلون افزایش یابد.

با وارد کردن ماشین آلات و دارایی‌هایی مانند کانتینرهای حمل و نقل و یا تخت بیمارستان‌ها به جهان متصل، اینترنت اشیاء راه‌های جدیدی را برای نظارت و مدیریت آن‌ها ارائه می‌کند که سبب ایجاد یک تجارت جدید می‌شود. یک مدیر می‌تواند در هر لحظه وضعیت کالاها یا مواد را در میان دستگاه‌ها، مراکز توزیع و حتی بر روی قفسه‌های فروشگاه مشاهده نماید. شرکت‌ها به وسیله نظارت ماشینی می‌توانند به طور آنی، جریان تولید کالاها را در کارخانه‌ها کنترل کنند و با نگهداری پیشگیرانه و عکس العمل سریع در هنگام بروز مشکل، از اختلال در روند عملیاتی جلوگیری نمایند. همچنین با جاسازی کردن حسگرهای هوشمند و محرک‌ها در ماشین آلات، آن‌ها می‌توانند جهت انجام کارهای خود برنامه‌ریزی شوند. استفاده گسترده از اینترنت اشیاء زمان‌بر خواهد بود، اما جدول زمانبندی نشان از سرعت همه گیر شدن استفاده از حسگرهای مینیاتوری و شبکه‌های بی‌سیم دارد.

اینترنت اشیاء این پتانسیل را دارد تا به طور سالانه تا سال ۲۰۲۵، تأثیر اقتصادی از ۲,۷ تریلون دلار تا ۶,۲ تریلون داشته باشد. برخی از کاربردهای مهم این فناوری، بهداشت و سلامت ، زیرساخت‌ها و خدمات بخش دولتی هستند که با کمک به اجتماع، بخش بزرگی از چالش‌های موجود را بر عهده می‌گیرند. به عنوان مثال نظارت از راه دور به طور بالقوه تفاوت زیادی در زندگی افراد مبتلا به بیماری‌های مزمن ایجاد می‌کند حال آن‌که انجام مراقبت‌های

[۷۵] connected world

بهداشتی فعلی برای چنین افرادی بسیار هزینه‌بر است. توانایی نظارت و کنترل شبکه‌های قدرت و سیستم‌های آب می‌تواند اثرات عمده‌ای بر حفاظت از انرژی، انتشار گازهای گلخانه‌ای و از دست دادن آب داشته باشد. با استفاده از حسگرهای جمع‌آوری اطلاعات برای ساده‌سازی عملیات، کارهای بخش دولتی مانند جمع‌آوری زباله می‌توانند بسیار بهتر انجام شوند. همچنین حسگرها می‌توانند جهت بهبود حفظ نظم اجتماعی مورد استفاده واقع شوند.

درک کامل پتانسیل‌های اینترنت اشیاء آسان نیست. برای دریافت ارزش این کاربردها، سازمان‌ها باید سیستم‌هایی داشته باشند که قابلیت جمع آوری حجم وسیع داده‌های ارسالی را داشته باشد. به عنوان مثال، با استفاده گسترده از RFIDها، برخی از شرکت‌ها می‌توانند صدها هزار نفر و یا حتی میلیون‌ها شیء را به طور آنی ردیابی کنند که به قابلیت‌های تحلیلی و هوش احتیاج دارد.

ادغام دنیای فیزیکی و دیجیتال نیز دارای پیامدهایی برای حفظ حریم خصوصی، امنیت و حتی چگونگی سازماندهی شرکت‌ها دارد. ضمن اینکه که اتصال داده‌ها این امکان را ایجاد می‌کند که ماشین‌ها از راه دور کنترل شوند و نیازی به دخالت انسان نباشد، راه را برای ورود متجاوزان و هکرها نیز باز می‌کند. به عنوان مثال داده‌های جمع آوری شده در مورد سلامت افراد می‌تواند مورد سوء استفاده قرار گیرند. حتی برای وسایل داخل خانه نیز این سوال که آیا حریم خصوصی و خودمختاری[۷۶] آن‌ها حفظ خواهد شد، وجود دارد. این مسائل قبل از آن که جامعه و تجارت شروع به استفاده از مزیت‌های اینترنت اشیاء کنند، باید پاسخ داده شوند.

### ۲-۵-۳-۱-تعاریف

منظور از اینترنت اشیاء، استفاده از حسگرها، محرک‌ها، و فناوری ارتباطات داده قرار داده شده در اشیاء فیزیکی برای ارتباط این اشیاء با هم به جهت ایجاد توانایی‌هایی همچون ردیابی یکدیگر، هماهنگی با هم، و یا کنترل آن‌ها در یک شبکه سراسری یا اینترنت است.

[۷۶] Autonomy

سه گام در کاربردهای اینترنت اشیاء وجود دارد: جمع‌آوری داده از شئ(به عنوان مثال داده‌ی موقعیت مکانی ساده شئ و یا اطلاعات پیچیده‌تر) گردآوری اطلاعات به منظور انتقال در شبکه داده و در نهایت انجام پردازش روی این اطلاعات(انجام بلافاصله پردازش روی آن‌ها و یا جمع‌آوری داده‌ها در طول زمان برای طراحی روش‌های بهبود فرایند)

اینترنت اشیاء می‌تواند به جهت ایجاد اعتبار به طرق مختلف استفاده شود. علاوه بر بهبود بهره‌وری در عملیات فعلی، اینترنت اشیاء می‌تواند انواع جدیدی از محصولات و خدمات و تجهیزات همچون حسگر کنترل از راه دور را ارائه دهد.

محدوده فناوری اینترنت اشیاء از یک تگ شناسایی ساده تا حسگرهای پیچیده و محرک‌ها است. محرک‌ها و دستگاه‌های پیشرفته چند حسگری که داده‌هایی از قبیل مکان، عملکرد، محیط زیست و شرایط را منتقل می‌کنند، در حال رایج شدن هستند. با فناوری‌های جدیدتر نظیر سیستم‌های میکرو الکترونیکی این امکان ایجاد می‌شود که در هر شئ (یا حتی انسان) از حسگرهای پیشرفته استفاده شود و از آن جایی که آن‌ها با استفاده از نیمه هادی‌ها تولید می‌شوند، قیمت آن‌ها به سرعت در حال کاهش است.

با دسترسی فزاینده سیستم‌های هوشمند اینترنت اشیاء، نه تنها شرکت‌ها را قادر به ردیابی جریان تولید محصولات و دارایی‌های فیزیکی می‌شوند، بلکه می‌توانند عملکرد کارکنان، مدیریت ماشین آلات و به طور کلی خط تولید را کنترل کنند. همچنین حسگرها می‌توانند در زیر ساخت‌ها جاسازی شوند؛ به عنوان مثال حسگرهای مغناطیسی در جاده‌ها می‌توانند تعداد و دفعات عبور وسایل نقلیه و یا گزارش لحظه‌ای از میزان ترافیک را ارائه دهند. البته انتقال داده‌ها به مرکز و پردازش آن (پردازش داده‌های حجیم) نیز بسیار مهم است.

کاربردهای اینترنت اشیاء شامل تنظیمات حلقه بسته‌ای است که فعالیت‌های آن به طور خودکار و بر پایه بسته‌های داده حسگرها است. برای مثال در صنایع پردازشی، سیستم‌های مبتنی بر حسگر می‌توانند به طور خودکار به سیگنال‌های ورودی واکنش نشان دهند و جریان پردازش را بر اساس آن تنظیم کنند. آن‌ها می‌توانند توسط تغییر نور به رنگ سبز، نحوه حرکت اتومبیل‌ها را به عابران اطلاع دهند و یا توسط صدای بوق پزشک را از وضعیت بیمارش از راه دور مطلع سازند.

در حال حاضر استفاده پایه‌ای از اینترنت اشیاء به خوبی در حال توسعه است. یکی از بزرگترین تجهیزاتی که تاکنون در این فناوری به خدمت گرفته شده است، RFIDها هستند که برای ردیابی جریان مواد اولیه، قطعات و کالاها در فرآیند تولید و توزیع است. برچسب های RFID سیگنال‌های رادیویی منتشر می‌کنند که می تواند به محل آن‌ها اشاره کند. به عنوان مثال وقتی یک محصول با چنین برچسبی عرضه می‌شود به راحتی می‌توان حرکت آن را از کارخانه تا بازار فروش کنترل کرد. به وسیله این اطلاعات شرکت‌ها می‌توانند زمان رسیدن محصول به بازار را کنترل کرده و نیازهای بازار را تشخیص دهند. پیگیری این جریان‌ها به شرکت‌ها این فرصت را می‌دهد تا زنجیره تأمین[۷۷] را محکم کنند و از هزینه‌های تولید و انبارسازی بیش از حد اجتناب نمایند. تگ‌های RFID در سیستم‌های E-ZPass نیز جهت کنترل جریان ترافیک و سرعت در جاده‌ها و پل‌ها استفاده می‌شوند.

در یک مثال دیگر شرکت FedEx برنامه‌ای پیشنهاد می‌کند که به مشتریان اجازه می‌دهد تا فرآیند ارسال بسته‌های خود را (با قرار دادن دستگاهی کوچک با اندازه یک گوشی موبایل در آن) به طور لحظه به لحظه ردیابی کنند. این وسایل شامل سیستم موقعیت‌یاب جهانی و حسگرهایی برای نظارت بر دما، رطوبت، فشار هوا و قرار گرفتن در معرض نور برای بسته‌های حاوی مواد بیولوژیکی و یا تجهیزات حساس الکترونیکی هستند. این نوع از در دسترس بودن مستمر داده برای شرکت‌هایی که عمل زنجیره پشتیبانی پیچیده و مداوم دارند، بدیهی است.

### ۲-۵-۴- عوامل بالقوه برای تسریع در استفاده از اینترنت اشیاء

اگرچه اینترنت اشیاء هنوز در مراحل اولیه‌اش می‌باشد اما در حال حاضر دارای گستره وسیعی از استفاده است و کاربردهای آن روزانه گسترش زیادی پیدا می‌کند. اینترنت اشیاء پتانسیل رفع نیازهای وسیعی، از جمله بهره‌وری منابع و مدیریت زیرساخت را دارد. شبکه‌های هوشمند برق، آب و شبکه‌های حمل و نقل نمونه‌هایی از این دست‌اند. صنایع آب و برق از جمله صنایع اولیه‌ای می‌باشند که از این تکنولوژی اقتباس کرده اند. حسگرها برای سیستم‌های شبکه هوشمند ضروری هستند چرا که به اپراتورها این امکان را می‌دهند تا میزان استفاده و عملکرد شبکه را در هر لحظه اندازه بگیرند. این بدین معنی است که به جای این‌که منتظر تماس مشتریانی شوند که برق آن‌ها قطع شده

[۷۷] Supply chains

است، شرکت‌های تولید برق می‌توانند نقطه قطع برق را تشخیص داده و با تغییر مسیر انتقال توان و یا تولید تجهیزات جدید، جریان برق را به نقطه قطع شدگی هدایت کنند. در حال حاضر حسگرهایی متصل به اینترنت وجود دارند که لرزه های روی پوسته زمین را قرائت کرده و بر جریان آب موجود در لوله‌ها نظارت دارند. در صنعت انرژی، حسگرها برای تعیین دقیق موقعیت مناطق ناشناخته دارای سوخت فسیلی مورد استفاده قرار می گیرند.

فناوری اینترنت اشیاء تأثیر مستقیم بر زندگی و سلامت انسان دارد. استفاده از سنسورها برای پیگیری عملکرد ورزشی و نمایش سلامتی فرد از زمینه‌های روبه رشدی است که توسط اینترنت اشیاء می‌تواند تقویت شود. به عنوان مثال چندین شرکت وجود دارند که در حال حاضر حسگرهای پوشیدنی می‌سازند. این حسگرها به مصرف کنندگان اجازه می‌دهد تا تعداد مایل‌هایی که راه رفته‌اند، نرخ ضربان قلبشان، و دیگر اطلاعات تولید شده طی ورزش را محاسبه کنند تا پس از آن برای مدیریت سلامت خود مورد استفاده قرار دهند. پزشکان در حال حاضر فرآیندی را تحت عنوان (capsule endoscopy) انجام می‌دهند که طی آن یک میکرو دوربین قرص شکل را که دارای قابلیت ارتباطی بی‌سیم است. از طریق دستگاه گوارش بیمار وارد بدن او کرده و تصاویر آن را به کامپیوتر منتقل می‌کنند.

چند پیشرفت تکنولوژیکی، باعث بهبود اثربخشی فناوری اینترنت اشیاء شده و هزینه‌های استفاده از آن‌را کاهش داده است.یکی اینکه قیمت تگ‌های RFID و حسگرها در حال کاهش است و دیگری پیشرفت‌های جدید مانند MEMS هستند که توانایی انجام امور بیشتری را ایجاد کرده‌اند. فروش حسگرها از سال ۲۰۱۰ هر ساله ۷۰ درصد رشد داشته است و پیشرفت در تکنولوژی باعث تولید حسگرهایی پیشرفته‌تر و مقرون‌به‌صرفه‌تر شده است. حسگرهای زیادی با انواع متنوع در داخل وسایل الکتریکی تعبیه شده‌اند تا با مدیریت انرژی مصرفی در آنها، برای مدت زمان طولانی‌تری مورد استفاده قرار گیرند.. تکنیک‌های کوچک سازی و تولید با حجم بالا این امکان را ایجاد کرده تا حسگرها را حتی در کوچکترین دستگاه‌ها نیز استفاده کنیم. به عنوان مثال یک گوشی هوشمند ممکن است دارای یک تراشه باشد که شامل یک حسگر موقعیت سنج، دماسنج و تعیین کننده مسیر باشد. در نهایت اینکه گسترش سریع شبکه‌های بی‌سیم سرعت بالا، با گسترش منطقه تحت پوشش اینترنت تلفن همراه، به هموار کردن راه جهت استفاده از اینترنت اشیاء کمک می‌کند.

### ۲-۵-۵- تأثیر اقتصادی بالقوه تا سال ۲۰۲۵

برآورد می‌شود که با بهره‌گیری از تنها نیمی از ظرفیت توانایی‌های اینترنت اشیاء تأثیر اقتصادی بالقوه آن تا سال ۲۰۲۵ از ۲,۷ تریلون دلار به ۶,۲ تریلون دلار درهر سال برسد. بیشترین میزان این تأثیرها در زمینه مراقبت‌های بهداشتی و تولید خواهد بود. تجزیه و تحلیل ما از کاربردهای فناوری اینترنت اشیاء در زمینه مراقبت‌های بهداشتی نشان می‌دهد که تأثیر اقتصادی آن از ۱,۱ تریلون دلار به ۲,۵ تریلون دلار درهر سال خواهد بود.

بزرگترین مزیت در مراقبت‌های بهداشتی را می‌توان بهبود بهره‌وری در درمان بیماران مبتلا به بیماری‌های مزمن دانست. با استفاده از حسگرهایی که علائم حیاتی بیماران را در خانه می‌خوانند، پرستاران و پزشکان می‌توانند از مشکلات در حال ظهور مانند یک قطره خطرناک در سطح گلوکوز یک بیمار دیابتی مطلع شوند. افزایش آگاهی بیماران در مورد چگونگی رسیدگی به مشکلاتشان در خانه و یا درمان آن‌ها به صورت سرپایی، باعث کاهش هزینه‌های اورژانس و بستری شدن غیر ضروری در بیمارستان‌ها می‌گردد. هزینه‌های معالجه بیماری‌های مزمن در حدود ۶۰ درصد از هزینه‌های مراقبت‌های بهداشتی را شامل می‌شود و هزینه‌های سالانه این بیماری‌ها تا سال ۲۰۲۵ درحدود ۱۵ تریلیون دلار خواهد بود. برآورد می‌شود که انجام نظارت از راه دور برای بیماران هزینه‌های درمان را از ۱۰ تا ۲۰ درصد کاهش می‌دهد. البته میزان کاهشی که رخ می‌دهد به میزان استفاده از این فناوری و میزان مقبولیت آن توسط بیماران بستگی دارد.

یکی دیگر از مزیت‌های کاربردی فناوری اینترنت اشیاء در مراقبت‌های بهداشتی می‌تواند بحث نظارت سلامت[۷۸] در بیمارستان‌ها باشد. داروهای تقلبی یکی دیگر از مشکلات مراقبت‌های بهداشتی است که می‌تواند با فناوری اینترنت اشیاء برطرف گردد. در حال حاضر بیش از ۷۵ میلیارد دلار از داروهای تقلبی در هر سال به فروش می‌رسد و این رقم هرساله ۲۰ درصد افزایش می‌یابد. به وسیله قرار دادن حسگرها در بطری داروها یا بسته آن‌ها می‌توان مصرف کنندگان را قادر به تعیین صحت داروی مورد استفاده نموده و از فروش داروهای تقلبی جلوگیری کرد. برآورد

[۷۸] Health monitoring

می‌شود که این روش می‌تواند به ۳۰ تا ۵۰ درصد از داروها اعمال شود و در ۸۰ تا ۱۰۰ درصد از مواقع موفقیت‌آمیز باشد.

در تولید نیز فناوری اینترنت اشیاء می‌تواند بهره‌وری عملیاتی را به روش‌های گوناگون بهبود بخشد. حسگرها می‌توانند در ماشین آلات مورد استفاده قرار گیرند و با به‌روز رسانی مداوم وضعیت تجهیزات میزان خرابی را کاهش دهند. حسگرها همچنین می‌توانند در کامیون‌ها و سایر ماشین‌الات سنگین به منظور ردیابی و مدیریت بهتر زنجیره منابع مورد استفاده قرار گیرند. آن‌ها می‌توانند برای نظارت بر جریان موجودی در طبقات کارخانه یا بین ایستگاه‌های کاری مختلف مورد استفاده واقع شوند. در ساخت اشیاء نیز می‌توان از حسگرها به جهت تعیین موقعیت دقیق اجزای یک شئ استفاده کرد و از انحرافات کوچک و خطاهای انسانی جلوگیری کرد.

تخمین زده می‌شود که افزایش بهره‌وری تولید از ۲,۵به ۵ درصد درهر سال به وسیله استفاده از فناوری اینترنت اشیاء مقدور خواهد بود. مجموع هزینه عملیاتی تولید جهانی در حال حاضر ۲۵تریلون دلار در سال است و می‌تواند به بیش از ۴۷ تریلون دلار تا سال ۲۰۲۵ برسد. با توجه به هزینه پایین استفاده از سنسوها و تقاضای زیاد برای روند بهینه سازی در تولید شاید ۸۰ تا ۱۰۰ درصد از تمام تولیدات تا سال ۲۰۲۵ به وسیله فناوری اینترنت اشیاء انجام شود. این امر به تأثیر اقتصادی بالقوه از ۹۰۰ میلیارد به ۲,۳ تریلون دلار در سال، تا سال ۲۰۲۵ منجر خواهد شد.

سیستم های شبکه برق هوشمند از دیگر کاربردهای اینترنت اشیاء هستند که دارای ارزش سالیانه بالقوه‌ای از ۲۰۰ میلیارد دلار تا ۵۰۰ میلیارد درسال ۲۰۲۵ خواهند بود. بخش عمده این تأثیر در کاربردهای مدیریت تقاضا خواهد بود بطوریکه هزینه استفاده در زمان اوج را کاهش می‌دهد. بسیاری از مصرف کنندگان تجاری از تولید کالا در زمان پیک مصرف انرژی اجتناب می‌کنند. زیرا هزینه‌های انرژی به بالاترین سطح خود می‌رسد و برخی از آن‌ها موافقت نامه‌های رسمی از شرکت‌های آب و برق دارند که هر وقت میزان تقاضا به حد معینی برسد مصرفشان را کاهش دهند. با استفاده از شبکه‌های هوشمند، مصرف‌کنندگان می‌توانند به شرکت های آب و برق این اجازه را بدهند که در سیستم‌ها و کاربردهای پرمصرف در زمان پیک بار به‌صورت خودکار میزان توان را کاهش دهند.

شبکه‌های هوشمند همچنین با ارائه اطلاعات لحظه‌ای در مورد وضعیت شبکه موجب کاهش هزینه‌های عملیاتی می‌شوند. از مزایای بالقوه استفاده از فناوری اینترنت اشیاء می‌توان به کاهش میزان قطعی و هدررفتن انرژی ازطریق

تنظیم ولتاژ و تعادل بار بین خطوط اشاره کرد. حسگرهای شبکه با نظارت بر شبکه و تشخیص مشکلات آن می‌توانند موجب جلوگیری از قطعی برق شبکه و یا کاهش هزینه‌های تعمیر و نگهداری آن شوند. کنتورهای هوشمند و دارای قابلیت ارتباط دوطرفه می‌توانند زمان قطع انرژی را کاهش داده و تشخیص علت قطع شدگی را سریع‌تر کنند.

اینترنت اشیاء مدیریت زیرساخت‌ها، سیستم‌ها و خدمات شهری همچون ترافیک، زباله، سیستم آب و امنیت عمومی بهبود می‌بخشد. حسگرهایی که بر الگوی ترافیکی نظارت دارند می‌توانند داده‌هایی را جهت بهتر کردن جریان ترافیک با تنظیم زمان چراغ‌ها و تغییر مسیر اتوبوس‌ها تولید کنند. در صورت رخداد حادثه حسگرها می‌توانند به طور خودکار جریان ترافیک را اطراف حادثه هدایت کرده و موجب کاهش هزینه تأخیر شوند. شهرهای لندن، سنگاپور و و هوستون با استفاده از این فناوری توانسته اند کاهش قابل ملاحظه‌ای در میزان رفت و آمدهای درون‌شهری ایجاد کنند. بر اساس این نمونه‌ها شهرها قادرند تا وسایل نقلیه موتوری را کاهش داده و از ۱۰ تا ۲۰ درصد در میزان رفت و آمدهای درون‌شهری صرفه جویی کرده و صدها میلیون ساعت در سال صرفه جویی زمانی داشته باشند.

شهرها همچنین می‌توانند با استفاده از فناوری اینترنت اشیاء مکانیزم جمع‌آوری زباله‌ها و میزان سلامت آب را بهبود ببخشند. به عنوان مثال در ایالات متحده شهرهای کلیولند[۷۹] و سینسیناتی[۸۰] در اوهایو هر خانواده دو سطل زباله و بازیافت مجهز به RFID دارد که این امکان را برای خدمه شهری محیا می‌سازد تا متوجه شوند آیا ساکنان زباله‌ها و سطل‌های بازیافت را در زمان معین در جای خود قرار داده‌اند یا نه. در سینسیناتی از طریق استفاده از این فناوری حجم زباله‌های مسکونی تا ۱۷ درصد کاهش و حجم زباله‌های قابل بازیافت تا۴۹ درصد افزایش داشته است.

شهرهای دوحه، ساؤپائولو و پکن همگی حسگرهایی را در لوله‌های آب، پمپ‌ها و سایر زیرساخت‌های آب برای نظارت بر شرایط و مدیریت بی آبی و شناسایی و تعمیر نشتی و یا تغییر فشار آب استفاده کرده‌اند. به طور متوسط این شهرها توانسته اند نشتی آب را بین ۴۰ تا ۵۰ درصد کاهش دهند. کنتورهای هوشمند به کاربر و یا مدیران اموال اجازه نظارت لحظه‌ای بر تقاضا و یا شناسایی نشتی را داده و موجب کاهش هزینه‌های مصرفی می‌شوند.

---

[۷۹] Cleveland

[۸۰] Cincinnati

کل تأثیرات اقتصادی باقوه شامل برنامه‌های ترافیکی، سطل زباله‌های هوشمند و سیستم‌های هوشمند آب در مناطق شهری باعث صرفه جویی از ۱۰۰ میلیارد دلار تا ۳۰۰ میلیارد دلار تا سال ۲۰۲۵ خواهند شد. این رقم با این پیش‌فرض است که تنها ۸۰ تا ۱۰۰ درصد از شهرهای توسعه یافته و ۲۵ تا ۵۰ درصد از شهرهای در حال توسعه تا این زمان می‌توانند دسترسی پیدا کنند..

اینترنت اشیاء همچنین می‌تواند به اجرای بهتر قوانین در شهرها کمک کند. به زودی قادر خواهیم بود با نصب حسگرهای ارزان قیمت در مراکز عمومی تصاویر و صداها را از محیط جمع‌آوری کرده و در مواقع لزوم به تجزیه و تحلیل آن‌ها بپردازیم. به عنوان مثال با تحلیل صدای گلوله از طریق چند سنسور می‌توان محل شلیک آن‌را تشخیص داد. این موضوع به طور بالقوه می‌تواند عملکرد پلیس را به سطح جدیدی از اثر بخشی برساند و هزینه‌های تشخیص جرم و جنایت را کاهش دهد. هزینه‌های اقتصادی جرم و جنایت ۵ تا ۱۰ درصد از تولید نا خالص داخلی در سراسر جهان است. حال اگر ۴ تا ۵ درصد از این هزینه‌ها حذف شود، توان بالقوه تأثیر اقتصادی آن می تواند در سال ۲۰۲۵، از ۱۰۰ میلیارد دلار تا ۲۰۰ میلیارد دلار در سال برسد.

در صنایع نفت، فلز و استخراج مواد معدنی، فناوری اینترنت اشیاء می‌تواند در پیدا کردن ذخایر معدنی و افزایش قابلیت بازیافت مؤثر باشد. ۵ تا ۱۰ درصد کاهش هزینه‌های عملیاتی از طریق استفاده از حسگرها در استخراج مواد پایه‌ای حاصل می‌شود.مجموع هزینه عملیاتی برای استخراج مواد معدنی، فلز و نفت در سال ۲۰۲۵، ۱۴تریلون دلار تخمین زده می‌شود. استفاده از فناوری اینترنت اشیاء در این صنایع می‌تواند بسیار زیاد( در حدود ۸۰ تا ۱۰۰ درصد ظرفیت) باشد.تأثیر اقتصادی بالقوه بر این صنعت در سال ۲۰۲۵ از ۱۰۰ تا ۲۰۰ میلیارد دلار در سال برآورد می‌شود.

فناوری اینترنت اشیاء در بخش کشاورزی این قابلیت را دارد که تأثیر قابل توجهی ایجاد کند. به عنوان مثال حسگرها قادر هستند رطوبت موجود در گیاهان را اندازه‌گیری کنند. حسگرهای خاک می‌توانند اطلاعات مورد نیاز در مورد چگونگی حرکت آب در مزرعه را جمع‌آوری و تغییر در میزان رطوبت خاک،کربن، نیتروژن و دمای خاک را اندازه‌گیری کنند. این داده‌ها به کشاورزان جهت بهینه‌سازی برنامه‌های آبیاری و اجتناب از آسیب محصول کمک می‌کنند. با استفاده از داده‌های حسگرها می‌توان بازده را ۱۰ تا ۲۰ درصد در سطح جهانی بالا برد. با فرض آن که

۲۵ تا ۵۰ درصد از مزارع این رویکرد را اتخاذ کنند، برآورد می‌شود که اینترنت اشیاء می‌تواند به طور بالقوه در سال ۲۰۲۵ به میزان ۱۰۰ میلیارد دلار صرفه اقتصادی برسد.

اینترنت اشیاء می‌تواند به رفع چالش‌های موجود در خرده فروشی کمک کند. برآورد شده است که خرده فروشان هر ساله معادل ۴ درصد از فروش خود را به خاطر کالاهایی که تمام شده و در انبار موجود نیست از دست می دهند. تا سال ۲۰۲۵ این زیان به میزان ۲۰۰ میلیارد دلار در سال خواهد رسید. برآورد می‌شود که ۳۵ تا ۵۰ درصد از این مقدار می تواند با استفاده از حسگرها و تگ‌هایی که میزان استفاده از هر کالا را تخمین می‌زنند و هرجایی که احتمال کمبود کالا رویت شد خبر می‌دهند، دوباره به سیستم بازگردد.

افزودن حسگر به خودرو برای جلوگیری از تصادف می‌تواند صرفه اقتصادی به میزان ۵۰ میلیارد دلار در سال، تا سال ۲۰۲۵ داشته باشد. این تخمین که براساس کاهش در میزان خسارت به اموال است، زمانی می‌تواند اتفاق افتد که سیستم‌های ترمز خودکار به‌صورت گسترده مورد استفاده قرار گیرند و از تصادفات سرعت-پایین[۸۱] به میزان زیادی جلوگیری به عمل آید.( تصادفات ناشی از سرعت-بالا که معمولا جراحات شدید و یا مرگ به دنبال دارد در تحلیل‌ها نیامده است.) برآورد می‌شود که با استفاده از فناوری اینترنت اشیاء ۲۵ درصد از میزان تصادفات سرعت-پایین کاهش خواهد یافت که معادل رقمی به میزان ۵۰ میلیارد دلار کاهش در خسارت اموال است.

در مجموع، اینترنت اشیاء تا سال ۲۰۲۵، تأثیری بین ۲,۷ تا ۶,۲ تریلیون دلاری در هر سال بر اقتصاد جهان خواهد گذاشت. جدول ۲-۵-۵-۱ اندازه تأثیرات اقتصادی اینترنت اشیاء را تا سال ۲۰۲۵ نشان می‌دهد.

**جدول ۲-۵-۵-۱ اثرات اقتصادی اینترنت اشیاء تا سال ۲۰۲۵ از دیدگاه مؤسسه Mckinsey**

| کاربردهای دسته بندی شده | تأثیر اقتصادی بالقوه تا سال ۲۰۲۵ برحسب تریلیون دلار در سال | میدان دید تخمینی در سال ۲۰۲۵ | توان بالقوه تخمینی قابل دسترسی در سال ۲۰۲۵ | توان بالقوه بهره‌وری یا بهره ارزشی در سال ۲۰۲۵ |
|---|---|---|---|---|
| مراقبت بهداشتی | ۱,۱-۲,۵ | • کاهش ۱۵,۵ تریلیون دلاری هزینه درمان بیماری‌های مزمن | • ۷۰-۸۰ درصد نفوذ تلفن همراه در بیماران که حجم مخارج مراقبت | • ۱۰-۲۰ کاهش در هزینه‌های درمان بیماری‌های مزمن از |

[۸۱] Low-speed

| | | | | |
|---|---|---|---|---|
| | | • کاهش ۴۰۰ میلیارد دلاری هزینه داروهای تقلبی، که ۴۰ درصد از آن‌ها قابل آدرس‌دهی با حسگرها هستند<br>• صرفه جویی در ۵۰ میلیون پرستار برای نظارت بیماران بستری<br>کشورهای پیشرفته:<br>۳۰دلار در ساعت<br>کشورهای در حال پیشرفت:<br>۱۵دلار در ساعت | بهداشتی را محاسبه می‌کنند.<br>• رویت داروهای تقلبی:<br>کشورهای پیشرفته :<br>۸۰-۵۰ درصد<br>کشورهای درحال پیشرفت:<br>۵۰-۲۰ درصد<br>• نظارت بر بیماران بستری<br>کشورهای پیشرفته:<br>۱۰۰-۷۵ درصد<br>کشورهای در حال پیشرفت:<br>۵۰-۰ درصد | طریق نظارت از راه دور سلامتی<br>• ۱۰۰-۸۰ درصد کاهش در داروهای تقلبی<br>• ۱-۰,۵ ساعت در روز زمان ذخیره شده برای هر پرستار |
| تولید | ۲,۳-۰,۹ | • کاهش ۴۷ تریلیون دلاری در هزینه‌های عملیاتی تولید جهانی | • ۱۰۰-۸۰ درصد همه تولیدات مجهز به برچسب RFID خواهند شد. | • ۵-۲,۵ درصد ذخیره در هزینه‌های عملیاتی شامل نگه‌داری و بازده ورودی |
| برق | ۰,۵-۰,۲ | • کاهش ۳۰۰۰۰-۲۷۰۰۰ TWh مصرف جهانی<br>• کاهش ۲۰۰ میلیارد دلاری هزینه روی خطوط انتقال<br>• کاهش ۳۰۰ میلیارد دقیقه در میزان قطع شدگی برق مصرف کنندگان | • ۵۰-۲۵ درصد از مصرف کنندگان می‌توانند از مدیریت انرژی استفاده کنند.<br>• ۵۰-۲۵ درصد از شبکه از طریق حسگرها نظارت خواهد شد<br>• ۱۰۰-۵۰ درصد از کنتور مصرف کنندگان خودکار خواهند شد. | • ۴-۲ درصد کاهش در اوج تقاضا در شبکه<br>• کاهش بار کل روی شبکه<br>• حفظ عملکرد و نگه‌داری، قطعی کمتر از طریق کنتورهای خودکار |
| زیرساخت شهری | ۰,۳-۰,۱ | • ۳۰۰-۲۰۰ ساعت صرفه جویی در زمان رفت‌وآمد کارکنان شهری در سال<br>• کاهش ۲۰۰ میلیارد دلاری در هزینه آب شهری<br>• کاهش ۳۷۵ میلیارد دلاری در هزینه مدیریت زباله | • ۷۰-۴۰ درصد از جمعیت شهری شاغل در شهرهایی زندگی می‌کنند که مجهز به زیرساخت هوشمند خواهند شد.<br>• ۷۰-۵۰ درصد از مناطق شهری بزرگ از زیرساخت آبی و مدیریت زباله هوشمند استفاده خواهند کرد. | • ۲۰-۱۰ درصد کاهش در میزان متوسط زمانی رفت‌وآمد در ترافیک و کنترل شلوغی.<br>• ۲۰-۱۰ درصد کاهش در مصرف آب و نشتی‌ها با استفاده از کنتورهای هوشمند و کنترل تقاضا.<br>• ۲۰-۱۰ درصد کاهش در هزینه مدیریت زباله |

| | | | | |
|---|---|---|---|---|
| امنیت | ۰,۱-۰,۲ | • کاهش ۶ میلیون دلاری در هزینه جرم | • ۵۰-۷۰ درصد از نظارت‌های پیشرفته به وسیله کشورها از طریق اینترنت اشیاء انجام خواهند شد. | • ۴-۵ درصد کاهش جرم به وسیله نظارت‌های بهبود یافته |
| استخراج منابع | ۰,۱-۰,۲ | • کاهش ۳,۷ تریلیون دلاری در هزینه‌های عملیات معدنی | • ۸۰-۱۰۰ درصد از همه استخراج‌های معدنی به اینترنت اشیاء مجهز می‌شوند. | • ۵-۱۰ درصد ذخیره در هزینه عملیات بهره‌وری |
| کشاورزی | ~۰,۱ | • صرفه جویی ۱,۳-۱,۲ تریلیون دلاری در هزینه تولیدات کشاورزی(گندم، ذرت، برنج، دانه‌های سویا، جو) | • ۲۰-۴۰ درصد از صنایع کشاورزی مجهز به سیستم‌های آبیاری پیشرفته و کشاورزی صحیح خواهند شد. | • ۱۰-۲۰ درصد افزایش در تولیدات با کاربردهای صحیح کود و آبیاری |
| خرده فروشی | ۰,۰۲-۰,۱ | • افزایش ۲۰۰ میلیارد دلاری درآمد بنابر گزارش ناشران سهام | • ۳۰-۸۰ درصد از خرده‌فروشی‌ها از تدارکات هوشمند بهره خواهند برد. | • ۱,۵-۲ درصد افزایش فروش‌ها |
| وسایل نقلیه | ~۰,۵ | • کاهش ۶۳۰ میلیارد دلاری در هزینه‌های پوشش حق بیمه | • ۱۰-۳۰ درصد از همه ماشین‌های بیمه شده به حسگرها مجهز خواهند شد. | • ۲۵ درصد کاهش در هزینه تصادفات اتومبیل‌ها با افزایش امنیت |
| جمع | ۲,۷-۶,۳ | | | |

## ۲-۵-۶- موانع و توانمندسازی‌ها

اینترنت اشیاء وعده بزرگی را می‌دهد اما هنوز تمام قسمت‌ها به نحوی در جای خود قرار نگرفته‌اند که تضمین دهند به میزان افزایش علاقه‌مندی به فناوری اینترنت اشیاء، میزان سرمایه‌گذاری و استفاده از آن نیز افزایش یابد. برخی مسائل فنی، مالی و نظارتی وجود دارند که باید حل شوند. به عنوان مثال باید ثابت شود مدل‌های کسب و کار مبتنی بر حسگرها سود و بازدهی بیشتری ایجاد می‌کنند.

از جنبه فناوری، هزینه حسگرها و محرک‌ها[۸۲] باید به میزانی کاهش یابد که استفاده از آن‌ها همه‌گیر شود. همچنین ارائه دهندگان تکنولوژی نیاز به توافق روی استانداردهایی دارند که قابلیت همکاری بین حسگرها، کامپیوترها و

[۸۲] actuators

محرک‌هارا داشته باشند. تا چنین استانداردهایی بوجود آیند، سرمایه‌گذاری در اینترنت اشیاء نیاز به تلاش برای ایجاد و حفظ سیستم‌های یکپارچه خواهد داشت. این پیشرفت‌ها همچنین نیاز به ایجاد نرم افزارهایی دارد که بتواند داده‌ها را آنالیز کرده و آن‌ها را به طریقی ارسال کنند که برای افراد معین و یا سیستم‌های خودکار مفید باشند.(به عنوان مثال محاسبه میزان دارو باید براساس داده‌های لحظه‌ای بیمار باشد.).

اینترنت اشیاء همچنین با موانعی چون، توجه به حریم خصوصی و حفظ امنیت روبه رو است که به اقداماتی از جانب تجارت‌ها و سیاست‌گذاران نیاز دارد . همچنان‌که کاربردهای اینترنت اشیاء پیچیده‌تر می‌شود و فعالیت‌های زیادی تحت کنترل سیستم‌های مبتنی بر حسگر قرار می‌گیرد، امنیت دادهها و شبکه قابل اطمینان این داده‌ها نیز اهمیت می‌یابد. . سیستم‌های کنترل ترافیک، برنامه‌های کاربردی مراقبت‌های بهداشتی، شبکه‌های هوشمند و فضای خرده فروشی همگی به وسیله استفاده از حسگرها قابل برنامه ریزی خواهند بود اما این نگرانی احتمالی وجود دارد که داده‌های تولید شده توسط این حسگرها در چه موارد دیگری ممکن است استفاده شود. به عنوان مثال این نگرانی وجود دارد که داده‌های مربوط به مراقبت‌های بهداشتی آیا برای انکار پوشش بیمه درمانی افراد مورد استفاده قرار خواهد گرفت؟ یا اینکه آیا هکرها می‌توانند داده‌های حسگرهای مربوط به حرکت خودروی شما را به منظور رصد اتفاقات شخصی  شما سرقت کنند؟

### ۲-۵-۷- تأثیرات و مفاهیم اینترنت اشیاء

اینترنت اشیاء یک مفهوم گسترده است که حتی تصور تمام زمینه‌های ممکن که این مفهوم قادر به تأثیرگذاری در آن‌ها می‌باشد، خود یک چالش است. کامپیوترها در حال حاضر قادر به دریافت داده‌ها از تقریبا هر نوع جسم فیزیکی هستند و ما را قادر به نظارت بر عملکرد ماشین آلات، اشیاء، زمین و حتی مردم می‌کنند. با استفاده از داده‌های این منابع، سیستم‌های کامپیوتری قادر به کنترل ماشین آلات و مدیریت ترافیک خواهند بود و یا حتی می‌توانند به یک بیمار دیابتی بگویند که زمان غذا خوردن است. این سرزمین جدید برای تقریبا همه افراد است، حتی کسانی که با درجه بالایی از تخصص فنی نیستند. تامین کنندگان امنیت، احتمالا یک لیست بلند از مشکلات این فناوری در ارتباط با حفظ حریم شخصی افراد می‌خواهند تا با حل آن‌ها اجازه‌ی بیان مزایای این فناوری را بدهند.

برای توسعه دهندگان فناوری و شرکت‌هایی که آن فناوری‌ها را هماهنگ می‌کنند اینترنت اشیاء پاداشی است که به دست آوردن آن ساده نخواهد بود. تولید کنندگان سخت افزار که حسگرها، محرک‌ها و وسایل ارتباطی را ارائه می‌کنند تحت فشار خواهند بود تا هم کارایی تولیداتشان را بهتر کنند و هم هزینه‌های ان‌ها را کاهش دهند. به عنوان مثال علی‌رغم سال‌های زیاد فروش در بازار، قیمت تگ‌های RFID همچنان برای بسیاری از تجارت‌ها که نیاز به تولید انبوه دارند بسیار گران می‌باشد. علاوه بر این چون سیستم‌ها شامل صدها هزار دستگاه، حسگر و سخت‌افزار هستند نیاز به وجود پشتیبانی، نگهداری و سازگاری خواهد بود. مشارکت‌های جدیدی بین شرکت‌های تولید کننده انواع حسگرها و تولید کنندگان ماشین آلات به جهت هوشمندسازی تولیدات انجام خواهد شد. برخی از شرکت‌هایی که دارای موقعیت مناسبی هستند ممکن است به عنوان تأمین‌کنندگان داده‌های بزرگ و نرم افزارهای تحلیلی عمل کنند که می‌تواند به تحلیل جریان عظیم داده‌ی تولید شده در فناوری اینترنت اشیاء کمک کند.

برای سیاست‌گذاران، فناوری اینترنت اشیاء فرصت‌ها و چالش‌های بزرگی به ارمغان می‌آورد. به عنوان عاملان زیرساخت و تامین کنندگان خدمات عمومی( اغلب شامل مراقبت‌های بهداشتی) دولت می‌تواند یکی از پذیرندگان اصلی اینترنت اشیاء باشد. این فناوری می‌تواند به شدت به کاهش هزینه‌ها و بهبود کیفیت خدمات کمک کند. ساکنان شهرها می‌توانند شاهد ترافیک روان، جمع آوری موثر زباله‌ها، کاهش جرم و جنایت و سیستم آب رسانی کارآمد باشند.

از لحاظ سیاست‌های عمومی، رهبران دولت نیاز به فهم روشن از خطرات حفظ حریم خصوصی در استفاده از فناوری اینترنت اشیاء دارند. قرار دادن حسگرها در هر جا به جهت مشاهده ترافیک در خیابان و یا کنترل مصرف انرژی در خانه یا محل کار نگرانی جدی در مورد حقظ امنیت و حریم خصوصی ایجاد می‌کند. اینترنت اشیاء ممکن است نیاز به وجود سطح بی‌سابقه‌ای از نظارت بر مردم داشته باشد که احتمالاً عموم مردم با این موضوع مخالفت می‌کنند.

سیاست گذاران در مواجهه با این مسائل نیاز به تمرکز جامع و در سطح جهانی دارند. آن‌ها نیاز به اجماع بر سر این موضوع که چه قوانین امنیتی و حمایتی باید در سراسر جهان اجرا شود دارند. متاسفانه سیستم‌های کامپیوتری و شبکه‌ها می‌توانند اهداف جنایتکاران، تروریست‌ها و یا حتی هکرها باشند. با حسگرها و شبکه‌های کنترل سیستم‌های

بحرانی، مانند شبکه برق، عواقب چنین حملاتی می‌تواند شدید باشد. رفع این چالش‌ها نیاز به فکر و برنامه ریزی وسیع و همکاری با بخش خصوصی دارد تا به ایجاد یک شرایط امن منجر گردیده و این شرایط امن با پیشرفت‌های فناوری به روز نگه‌داشته شود.

## ۲-۶- ۱۰ مزیت اینترنت اشیاء از دیدگاه مایکروسافت

[Create_the_Internet_of_Your_Things_Top_10_Benefits]

در این بخش ۱۰ دلیل نیاز تجارت به یک استراتژی برای سرمایه‌گذاری در IoT از دیدگاه مایکروسافت مطرح می‌شود که به به نوعی مزیت‌های آن نیز هستند (این مزیت‌ها توسط سرویس‌های Azure IoT شرکت مایکروسافت بدست می‌آیند):

۱- **شروع از اشیاء خود**: تنوع و فراوانی در اینترنت اشیاء نباید موجب دستپاچگی شود. نقطه نظر مایکروسافت نیز در این باره، تصور اینترنت اشیاء به عنوان اینترنت اشیاء خود، به جای سر در گم شدن در اشیاء بسیار زیاد موجود در جهان است. به همین منظور باید روی موضوع مناسب در تجارت که بازگشت سرمایه سریع دارد، متمرکز شد. در این حالت، شروع کار با عملیات، سیستم‌های متصل و دارایی‌های تجاری به منظور عملکرد بهتر به همراه نگهداری قابل پیش‌بینی و کاهش زمان خاموشی است.

۲- **بهره‌برداری بیشتر از دارایی[۸۳]های موجود**: از دارایی‌های موجود خود آغاز کنید و روی آن‌ها حساب باز کنید. مقدار کمی دارایی جدید اضافه کنید و آن‌ها را به سرویس‌های Azure IoT و ابر متصل کنید تا امکان صحبت آن‌ها با یکدیگر، با کارمندان و با مشتریان فراهم شود. همچنین با ابزارهای هوشمند تجاری، از داده‌هایی که این دارایی‌ها تولید می‌کنند استفاده کنید تا دید عمیق‌تری نسبت به نیازهای مشتریان و کارمندان داشته باشید.

۳- **کسب نتایج بزرگ با تغییرات کوچک**: IoT با شناسایی یک فرآیند، خط محصول یا مکانی که بیشترین ارتباط را با یک فرد دارد آغاز می‌شود و سپس با تغییراتی کوچک، به دنبال تأثیرات بزرگ است. برای

[۸۳] Asset

مثال، روبات‌های یک کارخانه را به وسیله سیستم‌های پشتیبان به یکدیگر متصل می‌کند و یک خط محصول با زمان فعال بیشتر ایجاد می‌نماید. یا به عنوان مثالی دیگر، تاریخ انقضا را به مجموعه داده‌های دارویی اضافه می‌کند تا موجب ذخیره هزاران دلار در تجویز داروی منقضی شود. یا در مثالی دیگر، یک دستگاه دستی را به سیستم دارایی‌ها متصل می‌کند، ضمن اینکه به طور آنی یک سرویس مشتری به فروش می‌رسد.

۴- **افزایش کارایی**: دانستن سلامت دارایی‌های تجاری مختلف می‌تواند یک چالش باشد. با این حال، وقتی از سرویس‌های Azure IoT برای اتصال و نظارت ساده سلامت دارایی‌ها استفاده شود، شرایط و عملکرد این دارایی‌ها در طول زمان قابل ردیابی خواهد بود. وقتی که یک فعالیت نیاز باشد، قواعد و هشدارها، سازمان یا تیم صحیح را آگاه می‌کند و بنابراین کارایی و فرآیندهای تجاری بهبود می‌یابد.

۵- **اتصال تمام دارایی‌ها**: ازدیاد سریع دارایی‌ها و دستگاه‌های متصل سبب ایجاد چالش‌های متعدد به دلیل گوناگونی پلتفرم‌ها و پروتکل‌ها می‌شود. با سرویس‌های Azure IoT، می‌توان دارایی‌های تجاری گوناگون امروزی را به یکدیگر متصل نمود. همچنین این سرویس‌ها، توانایی دریافت داده از تعداد بسیار زیادی از دستگاه‌ها و دیگر سیستم‌های تجاری را ارائه می‌دهند.

۶- **فراهم آوردن امکان نوآوری**: تجارت‌هایی که مرتب دارای به روز رسانی و تطبیق با نیازهای روز هستند، در رونق باقی می‌مانند. نظارت و تحلیل داده از منابع مختلف به طور تقریبا آنی نیز باعث نوآوری و ایجاد شرایط مناسب برای تجارت افراد می‌شوند. با قابلیت‌های یادگیری ماشین سرویس‌های Azure IoT، افراد می‌توانند از داده‌های قبلی برای یک مسأله جدید استفاده کنند و با ایجاد یک مدل و استفاده از آن، رفتار یا گرایش آینده را پیش‌بینی نمایند.

۷- **افزایش چالاکی**[۸۴]: آگاهی از داده‌ها می‌تواند به پاسخ سریعتر نسبت به رقابت‌ها، تغییرات زنجیره‌ای منابع، درخواست مشتریان و تغییرات شرایط بازار کمک کند. جمع‌آوری و تحلیل داده موجب آگاهی

[۸۴] Agility

سریع از گرایش‌های ایجاد و توسعه می‌شود که به وسیله آن، می‌توان فعالیت محصولات را تغییر داد، زمان‌بندی نگهداری و تعمیر را تنظیم کرد، یا مواد اولیه ارزان‌تر را مورد استفاده قرار داد. با اینترنت اشیاء، می‌توان زمان کمتری را اتلاف نمود و زمان بیشتری را به فعالیت پرداخت.

۸- **مقیاس‌پذیری توانایی‌ها**: ایده‌های جدید در هنگام کار با شرکا، تکنولوژی‌ها، دارایی‌ها و داده‌های جدید متولد می‌شوند. در این شرایط، می‌توان کارمندان و فناوری‌ها را با روش‌های جدید با یکدیگر در ارتباط قرار داد. فرصت‌های جدید باعث می‌شوند تا به جای تعمیر دارایی‌ها به تنظیم مناسب عملکرد آن‌ها در زمان طولانی پرداخته شود. مقایسه نتایج از فروشگاه‌های مختلف باعث می‌شود تا سرویس‌های موفق شناسایی شوند و سپس، آن‌ها را برای گسترش در سطح ملی انتخاب کرد. اینترنت اشیاء این امکان را فراهم می‌کند تا از کوچکترین نقطه به گسترش جهانی محصولات و سرویس‌ها دست یافت.

۹- **تبدیل تجارت**: داده‌ها قبل از آنکه به آگاهی و تأثیرات تجاری تبدیل شوند، چیزی بیش از صفر و یک نیستند. هنگامی که از داده‌های نظارت بر دارایی‌ها استفاده شود، با استفاده از تحلیل پیشرفته آن‌ها می‌توان نوآوری و تصمیم‌گیری را بهبود بخشید. همچنین پتانسیل تبدیل تجارت با ایجاد مدل‌های تجاری جدید و درآمد نیز قابل مشاهده است که پیش از این متصور نبود.

۱۰- **انتخاب یک شریک IoT معتبر**: مایکروسافت یک شرکت فناوری قابل اعتماد است. سرویس‌های Azure IoT باعث توامند ساختن افراد برای تبدیل داده از اشیاء به نتایج تجاری قابل اجرا می‌شود. مایکروسافت و شرکای آن، به افراد کمک می‌کند تا اینترنت اشیاء را در کار و تجارت روزانه خود قرار دهند که باعث رونق در کسب و کار می‌شود

## ۲-۷- ارکان اصلی رشد برای راه‌حل‌های آینده IoT

[http://iot-analytics.com/iot-infrastructure-providers-iot-hype/]

اجزای زیر، زیرساخت‌های غیر سخت‌افزاری IoT را تشکیل می‌دهند و به عنوان ارکان اصلی رشد برای راه‌حل‌های آینده آن محسوب می‌شوند:

۱- پلتفرم‌ها
۲- فناوری‌های دسترسی[۸۵]
۳- ذخیره‌سازی داده و پردازش
۴- تجزیه و تحلیل داده
۵- امنیت

این ۵ ستون یک بخش ضروری برای هر دستگاه متصل به اینترنت هستند. حال شرکت‌هایی که این زیرساخت‌های IoT را عملیاتی می‌کنند، بررسی نماییم.

### ۲-۷-۱- پلتفرم‌ها

یکی از راه حل‌های مختلف در مرحله اولیه و توسعه زیرساخت‌های IoT، پلتفرم mbed مربوط به شرکت ARM است که یک راه حل پایان به پایان ارائه می‌دهد. همانطور که IoT دارای هدف اتصال وسایل به یکدیگر است، پلتفرم mbed نیز یک لایه پایه از خدمات با سازگاری بین گره‌ها، خدمات ابری به همراه شبکه‌سازی IP، امنیت، لایه کاربرد و مدیریت دستگاه ایجاد می‌کند که همه آن‌ها برای توسعه کاربردهای IoT نیاز هستند. شرکت ARM نشان می‌دهد که این اجزا برای استفاده در اکثر موارد، متداول هستند. پلتفرم mbed تمام عناصر کلیدی لازم برای ساخت کاربردهای امن و کارآمد IoT را از طریق سیستم عامل mbed OS فراهم می‌کند. از دیگر موارد ذکر شده در این اکوسیستم نیز Xively، Thingworx، Axeda، Evrythng و 2lemetry هستند.

### ۲-۷-۲- فناوری‌های شبکه موبایل و دسترسی به موبایل

به عنوان یک ایده اولیه، فناوری IoT شامل اتصال دستگاه‌ها و انتقال داده‌ها است. در این میان، شرکت Telco company AT&T تلاش زیادی انجام می‌دهد تا موقعیت خود را به عنوان یک ارائه دهنده شبکه راهنما برای این اتصالات حفظ نماید. در حال حاضر، AT&T با بسیاری از شرکت‌های فعال دیگر در این زمینه مثل Amber Alert، GPS، Garmin، iLOC و غیره همکاری می‌کند تا تضمین و تأیید نماید که دستگاه‌ها می‌توانند در طیف IoT مورد

[۸۵] Access thechnologies

استفاده قرار بگیرند یا خیر. دیگر شرکت‌های مخابراتی بزرگ مثل Vodafone، Telefonica، یا Verizon نیز سرمایه‌گذاری‌های بزرگی در IoT کرده‌اند یا برای یک تغییر بزرگ در زیرساخت‌های IoT در حال برنامه‌ریزی هستند. همچنین Vodafone به همراه شرکای مختلف خود،تعدادی کاربرد IoT مانند شهر هوشمند، اشتراک خودرو و شهر امن را نیز در کنگره جهانی موبایل در سال ۲۰۱۵ ارائه کرده است.

لیست کاملی از تمام فیلم‌های نسخه نمایشی Vodafone را می‌توان در این آدرس اینترنتی پیدا کرد:

https://www.youtube.com/playlist?list=PL6253EF719F0738A8

اما شرکت Telcos به انطباق ضرورت راه‌حل‌های IoT می‌پردازد. بسیاری از کاربردهای IoT نیاز به مشخصات مختلف برای برقراری ارتباط و انتقال داده دارند. همچنین، توانی که برای عملگر نیاز است اغلب باید کم باشد بنابراین، شبکه‌های تلفن همراه تنها بخش از فناوری‌های دسترسی را تشکیل می‌دهند. بسیاری از فناوری‌های دیگر مانند Zigbee، Wifi,یا بلوتوث وجود دارد که همگی مشخصات خاصی از استفاده از توان، پهنای باند و محدوده را دارند. شبکه‌های LPWAN[۸۶] نیز یک جایگزین جالب برای استانداردهای ارتباطی بی‌سیم M2M هستند.

در این فضا امکان استفاده از شبکه WAN بدون مجوز، یک فرصت برای شرکت‌های کوچکتر ایجاد می‌کند تا با نوآوری‌های خود در بازار جایگاه اول را کسب کنند. همچنین در آینده‌ای نزدیک، می‌توان انتظار قوانین بسیاری را برای ایجاد امنیت بیشتر داشت.

### ۲-۷-۳- پردازش و ذخیره‌سازی/راه‌حل‌های ابری

جریان‌های داده که از دستگاه‌های با ظرفیت بالا سرچشمه می‌گیرند، باید به صورت امن و به نحوی که دوباره قابل دسترسی باشند و بتوان روی آن‌ها عملیات انجام داد، ذخیره‌سازی شوند. در حال حاضر تعداد کمی از ۲۰ شرکت برتر توسعه‌دهنده IoT، جزء شرکت‌هایی هستند که به رفع مسائل فضای ابری می‌پردازند. Microsoft Azure ، Amazon Web services، HP Helion، و Oracle Cloud برخی از راه‌حل‌های رقیب در این زمینه هستند.

[86] Low Power Wide Area Network

مزیت بیشتر شرکت‌های ارائه دهنده این راه‌حل‌های ابری زیرساخت IoT آن است که این راه حل‌ها می‌توانند مستقیماً در کاربردهای IoT استفاده شوند. به همین جهت، این شرکت‌ها با مقیاس‌دهی راه‌حل خود، در موقعیت قوی‌تری برای گسترش تجارت خود در فضای ابری قرار می‌گیرند. این شرکت‌ها تنها باید روی چالش‌های سازگاری ممکن تمرکز کنند که از انواع مختلف شبکه‌های دسترسی ناشی می‌شود.

### ۲-۷-۴- تجزیه و تحلیل

بسیاری از شرکت‌های ذکر شده در بالا که در زمینه حل مسائل فضای ابری کار می‌کنند، از یک دیدگاه، در دسته شرکت‌هایی هستند که در زمینه داده‌های عظیم[۸۷] فعالیت می‌کنند. اما داده‌های عظیم چیزی بیش از ذخیره‌سازی داده‌ها است. در واقع داده‌های عظیم، نیازمند عملکرد بالایی در تجزیه و تحلیل هستند. اگر چه برخی از شرکت‌های ذکر شده در بالا، پیشنهادهایی برای ارائه نوعی از تجزیه و تحلیل داده را دارند، اما شرکت‌های مهمی که بسته‌های تجزیه و تحلیل کامل‌داده را پیشنهاد می‌دهند شامل IBM، Oracle، SAP HANA و Teradata هستند.

ورای شرکت‌های ارائه دهنده تجزیه و تحلیل ترافیک، برخی پلتفرم‌های تجزیه و تحلیل داده وجود دارند که مدول‌های خاصی جهت تجزیه و تحلیل ارائه می‌دهند که از آن جمله می‌توان به تجزیه و تحلیل پیشگویانه[۸۸]، تجزیه و تحلیل جاری[۸۹]، استخراج یا پیش‌بینی داده[۹۰] را نام برد. در میان این شرکت‌ها می‌توان Splunk،1010data، Actian و Cloudera را نام برد.

اگر قرار باشد فقط یک توانمندساز برای IoT وجود داشته باشد، آن باید تجزیه و تحلیل داده باشد. اما با توجه به اینکه رقابت در این فضا درحال حاضر بسیار بالا است، سؤال اینجا است که چه تعدادی از این شرکت‌ها می‌توانند پیشرو در تولید زیرساخت IoT جهت تجزیه و تحلیل داده باشند.

---

[۸۷] Big Data

[۸۸] Predictive Analytics

[۸۹] Streming

[۹۰] Data Mining or Forecasting

### ۲-۷-۵- امنیت

در این مرحله مشکلات امنیتی که در زیرساخت‌های فضای سایبری وجود دارد، اعتبار راه‌حل‌های IoT را کاهش می‌دهد. حفظ حریم خصوصی دستگاه‌های شخصی و پتانسیل سوء استفاده از آن‌ها می‌تواند تبدیل به یک مانع عمده در توسعه فناوری IoT شود. مردم باید احساس کنند که داده آن‌ها به هنگام عبور از تجهیزات IoT امنیت دارد. شناسایی و ارائه راه‌حل‌های امنیتی این فرآیند را بسیار جلو خواهد برد. در این میان شرکت ARM به وضوح بر روی امنیت در سطوح مختلف از وسیله گرفته تا ذخیره‌سازی داده اصرار دارد.

شرکت‌هایی مانند Cisco در حال کار روی زیرساخت‌های امنیتی فناوری IoT هستند و در حال حاضر طرح‌هایی برای ارائه مدل امنیتی قوی برای IoT ارائه کرده‌اند. برای این منظور Cisco همه نوآوران، متفکرین و مجریان در زمینه امنیت را برای رفع چالش بزرگ امنیتی خود به کار گرفته است.

معیارهای مورد رقابت به صورت زیر هستند:

۱- امکان سنجی[۹۱]
۲- کاربری در حوزه‌های مختلف IoT
۳- بلوغ فنی[۹۲]

[۹۱] Feasibility

[۹۲] Technical maturity

# ۳- گزارشی از مراکز معتبر پژوهشی در زمینه اینترنت اشیاء

به جهت بررسی وضعیت اینترنت اشیاء در جهان، باید ابتدا نگاهی به مؤسسات، مراکز تحقیقاتی، شرکت‌ها، دانشگاه‌ها و آزمایشگاه‌های معتبر جهانی بیاندازیم تا رویکرد کلی تحقیقات در این زمینه را شناسایی کنیم. این بررسی، یک شناخت اولیه در مورد وضعیت جهانی و رویه مراکز معتبر پژوهشی در زمینه اینترنت اشیاء ارائه می‌دهد که با استفاده از آن، می‌توان موضوعات تحقیقاتی مهم را در اینترنت اشیاء پیدا کرد تا بحث امنیت (که طبیعتا یکی از مهمترین موضوعات و چالش‌ها در IoT است) را در این موضوعات مورد بررسی قرار داد. به همین جهت، این فصل به بررسی برخی از این مراکز معتبر پژوهشی می‌پردازد.

## ۳-۱- مؤسسات و مراکز تحقیقاتی

در این بخش به معرفی برخی مؤسسات و مراکز تحقیقاتی مهم در زمینه اینترنت اشیاء می‌پردازیم.

### ۳-۱-۱- IERC[۹۳]

[IERC Cluster Book]

IERC یک مرکز تحقیقاتی اختصاصی برای IoT است؛ که هدف آن طراحی و اجرای پروژه های متعدد در زمینه رفع چالش‌های پیش روی توسعه فناوری IoT در سطح جهان و در نهایت ارائه یک تعریف و دیدگاه ثابت برای این فناوری است که کاملا مطابق با استانداردهای اروپا باشد. از جمله اهداف اصلی IERC را می توان به صورت زیر برشمرد:

۱- ایجاد یک چارچوب همکاری و چشم انداز پژوهش برای فعالیت IoT در اروپا و تبدیل شدن به یک دروازه بزرگ ورود اطلاعات و تحقیقات در زمینه این فناوری.

۲- تعریف یک استراتژی بین المللی برای همکاری در حوزه IoT و ایجاد نوآوری در زمینه‌های گوناگون مرتبط با این فناوری و مشاهده و کنترل روی انواع نوآوری‌هایی که در سطح جهانی صورت می‌گیرد.

۳- هماهنگ نمودن نوآوری‌های انجام شده در حوزه IoT با پروژه‌های متفاوت در ICT

[۹۳] European Research Cluster on the Internet of Things

۴- ایجاد و سازمان‌دهی بحث، گفت و گو، و کارگاه‌های آموزشی که منجر به درک بهتر از فناوری IoT و فناوری‌هایی همچون 5G و فناوری ابری شود.

اما پروژه‌هایی که مرکز IERC در حال حاضر مشغول انجام آن‌ها است را می توان به پنج بخش زیر تقسیم کرد:

۱- روش ها و مدل‌های معماری IoT

۲- تحقیق و بررسی پروژه‌های در حال اجرا در سطح دنیا در حوزه IoT به منظور کشف اهداف و دستاوردهای آن‌ها

۳- مسائل مربوط به حریم خصوصی و امنیت در IoT

۴- ایجاد بستری برای استفاده از خدمات و همکاری‌های مشترک با سایر کشورها و مؤسسات

۵- مسائل و مدل های مربوط به هر حکومت و قوانین خاص آن

### ۳-۱-۲- OWASP[۹۴]

[https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=Manufacturers]

این مؤسسه، یک انجمن باز[۹۵] است که به طور اختصاصی سعی در ایجاد امنیت در تجارت، توسعه، برنامه‌های کاربردی و اهداف سازمان‌ها و ادارات دارد. این انجمن قصد دارد تا با ایجاد امنیت در نرم‌افزارها و تجهیزات مورد استفاده بشر، با نزدیک کردن وسایل هوشمند و تجهیزات قابل برنامه‌ریزی به زندگی حالت مکانیکی بدهد. اما تحقیقات این مؤسسه در زمینه IoT در سال ۲۰۱۴ منجر به ایجاد پروژه‌ای امنیتی به نام OWASPInternet of Things Top 10 شد که هدف آن بررسی و رفع ۱۰ مشکل امنیتی است که در دستگاه‌های هوشمند وجود دارند. این مؤسسه مشکلات مذکور را به صورت زیر لیست می‌کند:

۱- رابط کاربری وب نا امن

۲- صدور مجوز و احراز هویت نا امن

---

[۹۴] Open Web Application Security Project

[۹۵] Open community

۳- خدمات شبکه نا امن

۴- عدم استفاده از رمزنگاری برای انتقال داده‌ها

۵- نگرانی‌های حریم خصوصی

۶- رابط کاربری ابری نا امن

۷- رابط کاربری همراه نا امن

۸- توانایی پیکربندی امنیتی ناکافی

۹- نرم‌افزار/سفت‌افزار نا امن

۱۰- امنیت فیزیکی ضعیف

### ۳-۱-۳- Council

[http://www.theinternetofthings.eu]

از نظر کمیسیون مجلس اروپا، کمیسیون اقتصادی و اجتماعی و کمیته مناطق، فناوری IoT یک طرح عملی برای اروپا است. اگرچه این فناوری هنوز یک واقعیت ملموس نیس، اما یک چشم‌انداز از تعدادی فناوری است که همراه با هم می‌توانند در ۵ تا ۱۵ سال آینده به شدت جوامع ما را تغییر دهند.

با اتخاذ رویکرد پیشگیرانه، اروپا می‌تواند نقشی هدایتگر در شکل دادن به نحوه کار IoT بازی کند و مزایای مرتبط آن را از نظر رشد اقتصادی و رفاه فردی صاحب شود. غفلت از این کار به معنی از دست رفتن فرصت است. لذا این موضوع، اروپا را مجبور به استفاده از فناوری می‌کند که با برخی از مسائل اصلی مانند حریم خصوصی و اطلاعات شخصی در تعارض است.

به وسیله راه‌اندازی برخی از اقدامات، کمیسیون پارلمان اروپا در نظر دارد تا به عنوان نیروی محرک فناوری قرار بگیرد، و پارلمان اروپا، گروه Council و همه ذینفعان را به کار مشترک برای رسیدن به این اهداف دعوت کند. با توجه به این موضوع، اثبات شده است که اینترنت اشیاء یک طرح عملی برای اروپا است. کمیسیون پارلمان اروپا معتقد است که یک مکانیزم با چند ذینفع در اروپا بر سر این موضوع وجود دارد که نیازمند تدوین سیاست اتحادیه اروپا برای پیگیری و انجام اقدامات مورد نیاز است.

از این رو نیاز به راه‌اندازی یک گروه متخصص در زمینه اینترنت اشیاء و تعریف وظایف و ساختار آن وجود دارد. گروه Council نقش این گروه را بازی می‌کند. این گروه گفت و گو میان ذینفعان را تسهیل می‌کند.

### ۳-۱-۳-۱-مأموریت گروه Council

فناوری IoT یک تغییر در هستی شناختی است. مفاهیم ما از انسان و موجودیت بر پایه دوگانگی موضوعیت و شیء است. IoT قسمت سومی را به معادله اضافه می‌کند که یک پایگاه داده است.

اینترنت اشیاء می‌تواند بهترین بازخورد ممکن در سلامت جسمی و روانی، بهترین اندازه‌گیری بر اساس کنترل لحظه‌ای برای تشخیص منابع، بهترین تصمیم گیرنده بر اساس داده‌های واقعی و اطلاعات از منابع باز باشد.

اینترنت اشیاء در ذات خود رابطه‌ای بین اجزای زیر است:

- BAN (شبکه محدود به بدن): کمک کننده به شنود در محیط، لباس هوشمند و غیره
- LAN (شبکه محلی): کنتور هوشمند
- WAN (شبکه گسترده): دوچرخه، ماشین، قطار، اتوبوس و هواپیمای بدون سرنشین
- VWAN (شبکه بسیار گسترده): مغز شهر به عنوان خدمات الکترونیکی دولت‌ها

هر روشی که قابلیت ردیابی، پایداری و امنیت را عملی کند اهمیت بالاتری خواهد داشت. گروه Council برای ساخت جامع‌تر و نوآورانه‌تر IoT به "راه‌حل برنده[۹۶]" اعتقاد دارد، به نحوی که در تضاد با نوآوری‌های اجتماعی و امنیت نباشد و به وسیله پیدا کردن راهی برای ترکیب این دو ضرورت در یک چشم انداز وسیع‌تر که کاربر پسند نیز باشد، هدف خود را دنبال می‌کند. شاید این راه‌حل، یک راه‌حل مثبت و یک گام منطقی در تاریخ استفاده از اشیاء، وسایل، محیط زیست و چالش‌هایی که ما همه روزه با آن‌ها روبه‌رو هستیم، باشد.

گام بعدی تغییری است که گروه Council در مدل ادراکی روزانه خود از دانش در مؤسسات و محیط‌های رسمی شاهد خواهد بود. در حال حاضر ما می‌توانیم کارها و وظایف خود را با استفاده از IoT و در غالب اشیاء، خانه‌ها و شهرهای هوشمند انجام می‌دهیم. هدایتگر اصلی در پشت اشیاء هوشمند، مدیریت موجودی و ضدسرقت است. خانه

[۹۶] Winning solution

هوشمند به این معنی است که ما به سادگی قادریم تا بدون کمک دیگران امور خود را در داخل خانه انجام داده و مدت طولانی‌تری در خانه بمانیم، چرا که این خانه است که برای ما برنامه‌ریزی کرده و کارهای ما را انجام می‌دهد. به عنوان مثال زمان ورزش کردن را به ما اطلاع می‌دهد.

تشخیص چهره، حسگرهای زیستی و معماری هوشمند همگی یک شهر هوشمند و مطابق با برنامه‌های طراحان ایجاد می‌کنند، و هرگز به معنی ترس بیشتر، غیر انسانی‌تر، و تجارت و نوآوری کمتر نیستند.

گروه Council سناریوها و برنامه‌های کاربردی واقعی را که خصوصیات بنیادی دموکراسی را تشخیص می‌دهند، بررسی می‌کند و راه‌حلی برای تسهیل همبستگی و سازماندهی اشیاء ارائه خواهد داد.

### ۳-۱-۳-۲- Council به عنوان یک شریک علمی برای کنفرانس "IoT 2010 Europe"

رهبران تجاری، طرفداران حقوق مصرف کننده، سیاست‌گذاران و کارآفرینان با ملحق شدن به هم تحت یک کنفرانس، اثر نقشه راه IoT در سال‌های آتی را در چگونگی تعاملات ما با جهان واقعی و مجازی بررسی کردند. این کنفرانس به نگرانی‌های موجود از نحوه توسعه جامعه اروپا و کشف چالش‌های بالقوه آن پرداخته است و موضوعات مطرح شده در آن به صورت زیر است:

- چگونه فناوری IoT شهروندان را در انجام امور فردی خود توانمند می‌کند؟
- چه نوآوری‌ها و توسعه‌هایی از فناوری IoT دیده خواهد شد؟
- چه چالش‌های امنیتی، به ویژه در دسترسی غیر مجاز و افشای ناخواسته داده‌ها ممکن است توسط فناوری IoT ایجاد شود.
- چگونه ما می‌توانیم رقابت مؤثر در فناوری IoT را تشویق کنیم؟
- چگونه می‌توانیم یک شرایط مناسب برای تشویق سرمایه‌گذاری ایجاد کنیم؟
- چگونه می‌توانیم به تبادل بهترین درس‌ها و تمرین‌ها با خارج از اروپا بپردازیم؟

http://www.theinternetofthings.eu/internet-of-things-what-is-it%3F

### ۳-۱-۳-۳- اینترنت اشیاء از دیدگاه Council

در حال حاضر تمیز دادن دو بلوک اصلی اندیشه در فناوری IoT امکان‌پذیر است. اولی، چارچوب انفعالی از ایده‌ها و فکرهایی است که IoT را به عنوان لایه‌ای از اتصال دیجیتال در بالای زیر ساخت‌ها و اشیاء موجود می‌بینند. در این چارچوب، IoT به عنوان یک مجموعه قابل مدیریت از تحولات همگرا در زیرساخت‌ها، خدمات کاربردها و ابزارهای حکومتی در نظر گرفته می‌شود. دومی یک چارچوب از ایده‌ها و طرز فکرهایی است که IoT را به عنوان یک همگرایی به شدت مخل که قابل مدیریت به واسطه ابزارهای فعلی نیست، در نظر می‌گیرد و قصد دارد آنچه به عنوان داده است را تغییر دهد.

فناوری IoT دنیایی را متصور است که در آن هر چیزی می‌تواند به صورت آنالوگ و دیجیتال باشد و IoT، روابط ما با اشیاء و نیز روابط اشیاء با هم را به نحوی دیگر سازماندهی می‌کند. هر شیء که یک برچسب RFID داشته باشد، نه تنها به شما بلکه به همه دستگاه‌های مجهز به خواننده RFID، به دیگر اشیاء، رابط‌ها یا واسط‌های پایگاه داده گزارش می‌دهد.

شاید این فناوری راه حلی مثبت و گامی منطقی در تاریخ اشیاء و وسایل و محیط زیست برای رفع چالش‌هایی که ما همه روزه با آن‌ها روبه رو هستیم، باشد.

چه می‌شود اگر از طریق فناوری IoT بتوانیم یک لایه از داده ایجاد کنیم که برای همه در دسترس باشد و از طریق آن افراد بتوانند برای خود تصمیم بگیرند که آن‌ها مایل به پرداخت چه هزینه‌ای هستند، چه بازخوردی از کمک‌های داوطلبانه خود می‌گیرند، و با افراد دیگر از سایر نقاط جهان چگونه پول خود را به اشتراک می‌گذارند.

### ۳-۱-۳-۴- سؤالات در مورد فناوری IoT

فناوری IoT با وعده‌های شگفت‌اگیز از اتصال فراگیر و بی‌پایان اشیاء و ایجاد اتوماسیون ظهور کرده است. این فناوری نیازمند زیرساخت‌های فیزیکی، دیجیتالی و مجازی دستگاه‌ها و اشیاء است و قصد مدیریت همه چیز را برای ما و از طریق خود ما و از طریق شبکه‌های انرژی و ترافیک دارد.

سناریو هوشمندانه فناوری IoT اشکال جدیدی از روابط میان خودمان با دیگران و محیط اطراف ما را معرفی می‌کند. اشیاء هوشمندی که ما در اختیار خواهیم داشت، راه‌های جدیدی را برای زندگی ما تعیین خواهند کرد. این وسایل، تعاملات اجتماعی، یادگیری و تصور ما را از آنچه به عنوان انسان است، تغییر خواهند داد.

گروه Council، برای شروع یک بحث باز روی اهداف اساسی IoT و کشف چالش‌های اجتماعی و اخلاقی آن فعالیت خود را با سؤالات زیر از دیگران آغاز نمود:

- تعریف شما از فناوری IoT چیست؟
- چرا نیاز به فناوری IoT داریم؟
- چه کسی از این فناوری بهره‌مند خواهد شد؟
- چه کسی تصمیم می‌گیرد که ما به آن نیاز داریم و چرا؟
- چه چیزی را می‌توانیم از گرایش خودمان به این فناوری انتظار داشته باشیم؟
- آیا ما به طور منطقی قادر به تفسیر تجارب و احساسات خودمان در قالب الگوریتم‌ها هستیم؟
- آیا همانطور که فناوری دقیق می‌شود، توانایی ما به فکر، احساس و عمل تحت تأثیر قرار می‌گیرد؟
- چه تصمیماتی می‌توانند یا نمی‌توانند به اشیاء هوشمند واگذار شوند؟
- آیا اطلاعات بیشتر، مساوی با دانش و توانمندی بیشتر است؟
- ارزش‌ها و هنجارهای چه کسی در دستگاه‌های ما جاسازی شده است؟
- ما تا چه میزان به یکدیگر وابسته خواهیم شد، وقتی که به عنوان اشیایی در فناوری IoT باشیم؟
- آیا برنامه‌های فناوری IoT نابرابری‌ها و اختلالات اجتماعی موجود و یا در حال ظهور را افزایش می‌دهد؟
- من از طراحی این فناوری به طور پیش‌فرض چه می‌خواهم؟
- چه کسی بر این فناوری حکومت خواهد کرد؟
- آیا قدرت کافی برای مقامات مسؤول به منظور برقراری تعادل در بین شرکت‌هایی که قصد توسعه فناوری IoT را دارند، وجود دارد؟

- چگونه ما باید کار در شهرهای هوشمند را مدیریت کنیم تا اطمینان حاصل شود که ارزش‌ها و هنجارهای تعریف شده در دستگاه‌های متصل هوشمند، واقعاً منعکس کننده نیازها، انتظارات، نگرانی‌ها و اولویت‌های شهروندان هستند؟
- چگونه فناوری IoT تحت فشار ترکیبی از نانو و بیوتکنولوزی، داده‌های بزرگ و فضای ابر تکامل می‌یابد؟

### ۳-۱-۴- سایر

در حال حاضر مؤسسات، دانشگاه‌ها و گروه‌های پژوهشی بسیاری در سراسر جهان در حال مطالعه روی IoT و طراحی استانداردهای متفاوت جهت اتصال اشیاء و انتقال اطلاعات میان آن‌ها هستند، که از جمله مهم‌ترین این مراکز می‌توان به ETSI[۹۷]، IETF[۹۸]، IEEE[۹۹]، OMG[۱۰۰]، OASIS[۱۰۱]، OGC[۱۰۲]، IoT-A، OneM2M، OSIoT، IoT-GSI، ISA، W3C و Eclipse اشاره کرد. در ادامه به برخی از استانداردها و پروتکل‌های مهم، رایج و مرتبط با IoT اشاره می‌کنیم که توسط این مراکز ارائه شده‌اند.

- SOAP[۱۰۳]: یک پروتکل برای تشخیص تبادل اطلاعات در شبکه‌های کامپیوتری.
- IPv6: یک پروتکل در لایه اینترنت است که برای انتقال داده‌ها در شبکه‌هایی با چند IP مورد استفاده قرار می‌گیرد.
- 6LOWPAN[۱۰۴]: نوع خاصی از پروتکل IPV6 است که با استاندارد IEEE 802.15.4 منطبق شده است. نرخ انتقال در این پروتکل 250kbps است.

---

[۹۷] European Telecommunication Standards Institute

[۹۸] Internet Engineering Task Force

[۹۹] Institute of Electrical and Electronics Engineers

[۱۰۰] Object Management Group

[۱۰۱] Organization for the Advancement of Structured Information Standards

[۱۰۲] Open Geospatial Consortium

[۱۰۳] Simple Object Access Protocol

[۱۰۴] IPV6 over Low Power Wireless Personal Area Networks

- UDP[۱۰۵]: این پروتکل مورد استفاده در شبکه‌های IP دارای سرور/کاربر[۱۰۶] است.
- DTLS[۱۰۷]: این پروتکل به برنامه‌های سرویس دهنده و سرویس گیرنده اجازه می‌دهد تا به نحوی با هم ارتباط برقرار کنند که از استراق سمع، دستکاری یا جعل پیام جلوگیری شود.
- MQTT[۱۰۸]: این پروتکل امکان انتقال پیام‌ها را به طریقی بسیار سبک فراهم می‌کند؛ که برای ارتباط با مکان‌های دور بسیار مفید است.
- COAP[۱۰۹]: این پروتکل جهت استفاده در لایه کاربرد طراحی شده است. در این پروتکل الزامات تخصصی از قبیل پشتیبانی چند بخشی و سادگی رعایت شده است.
- SMCP[۱۱۰]: این پروتکل بر پایه پروتکل COAP است و بسیار برای جاسازی در تجهیزات مناسب است.
- XMPP[۱۱۱]: این پروتکل جهت انتقال طیف گسترده‌ای از برنامه‌های کاربردی از جمله پیام‌های فوری، چت و تماس‌های صوتی و تصویری مناسب است.
- AMQP[۱۱۲]: این پروتکل یک پروتکل لایه کاربرد است. از ویژگی‌های این پروتکل می‌توان به مسیریابی و صف‌بندی و امنیت پیام‌های ارسالی اشاره کرد.
- LLAP[۱۱۳]: این پروتکل در واقع یک پیام ساده کوتاه است که بین اشیاء هوشمند و با استفاده از متن معمولی ارسال می‌شود.

---

[۱۰۵] User Datagram Protocol

[۱۰۶] Server/client

[۱۰۷] Datagram Transport Layer Security

[۱۰۸] Message Queuing Telemetry Transport

[۱۰۹] Constrained Application Protocol

[۱۱۰] Standard Marine Communication Phrases

[۱۱۱] Extensible Messaging and Presence Protocol

[۱۱۲] Advanced Massage Queuing Protocol

[۱۱۳] Lightweight Local Automation Protocol

- SSI[۱۱۴]: یک پروتکل ساده ارتباطی که برای انتقال داده بین کامپیوترها یا سنسورهای هوشمند مورد استفاده واقع می‌شود.
- SensorMl: وظیفه این پروتکل فراهم نمودن استانداردها و استفاده از رمزنگاری XML برای توصیف سنسورها و فرآیندهای اندازه‌گیری است.
- IEEE 1451: یک خانواده از استانداردهای هوشمند است که وظیفه آن‌ها توصیف مجموعه‌ای از رابط‌های ارتباطی باز، مشترک و مستقل از شبکه[۱۱۵] برای اتصال سنسورها به ریزپردازنده‌ها می‌باشد.
- IEEE 1888.3-2013: یک استاندارد امنیتی برای شبکه کنترل ارتباطات است.
- IEEE 1905.1-2013: استانداردی برای شبکه کردن تجهیزات خانگی ناهمگن است.
- IEEE 80216p-2012: استاندارد مورد استفاده در سیستم‌های دسترسی بی‌سیم است.
- IEEE P1828: استانداردی برای سیستم‌های با قطعات مجازی است.
- IEEE P1856: یک چارچوب برای مدیریت سیستم‌های الکترونیکی است.
- IEEE 802.15.4: استانداردی جهت مشخص کردن لایه فیزیکی برای شبکه‌های بی‌سیم است.
- NFC: یک استاندارد با نرخ انتقال داده 424kbps جهت انتقال در شبکه‌های حسگر بی‌سیم است.
- ANT: یک پروتکل اختصاصی برای شبکه‌های حسگر بی‌سیم است و شامل قوانین تعریف شده ورود و خروج داده و تشخیص خطا است.
- Bluetooth: دارای نرخ ارسال اطلاعات ۳ مگابیت برثانیه و تا حداکثر ۱۰۰ متر است. هر وسیله‌ای که از این نحوه ارتباط استفاده می‌کند، دستورالعمل خاص خود را دارد.
- ZigBee: این پروتکل از استاندارد IEEE 802.15.4 استفاده می‌کند و حداکثر تا فاصله ۲۰۰ متر امکان برقراری ارتباط دارد. همچنین از رمزنگاری AES نیز استفاده می‌کند.

---

[۱۱۴] Simple Sensor Interface

[۱۱۵] Network- independent

- EnOcean: یکی از انواع فناوری‌های بی‌سیم است که در اروپا با فرکانس ۸۶۸ مگاهرتز و در آمریکا با فرکانس ۳۱۵ مگاهرتز کار می‌کند. محدوده انتقال آن نیز به ۳۰ متر می‌رسد.
- Dash 7: برپایه استاندارد ISO 18000-7 کار می‌کند. محدوده انتقال آن از ۱۰ تا ۱۰۰ کیلومتر و نرخ انتقال آن به صورت پویا از ۲۸ تا ۲۰۰ مگابیت بر ثانیه تنظیم می‌شود.
- WiMax: برپایه استاندارد IEEE 802.16 برنامه‌ریزی شده است. محدوده انتقال آن برای ایستگاه‌های ثابت تا ۵۰کیلومتر و برای ایستگاه‌های متحرک بین ۵ تا ۱۵ کیلومتر متغییر است و نرخ انتقال آن نیز ۴۰مگابیت در ثانیه است.

## ۳-۲- ۱۵ شرکت سهامی معتبر در زمینه IoT

[http://iot-analytics.com/15-internet-of-things-stocks]

اگر فردی در سال ۱۹۸۶، دو هزار دلار در سهام مایکروسافت سرمایه گذاری می‌کرد، ۱۳ سال بعد یک میلیونر می‌شد. از نقطه نظر سرمایه‌گذار سؤالی که در زمینه IoT مطرح می‌شود، چنین است: کدام شرکت می‌تواند در زمینه IoT فرصتی همچون فرصتی که مایکروسافت در زمینه نرم‌افزار ایجاد کرد، ایجاد نماید؟ چگونه می‌توان در سهام IoT سرمایه‌گذاری انجام داد؟

در این بخش لیستی از ۱۵ شرکت که تجارت قابل ملاحظه‌ای در IoT دارند، به طور عمومی لیست شده است و هنوز در این بین، شرکت‌های بزرگ قرار ندارند.

### ۳-۲-۱- سهام‌های IoT در زمینه سخت‌افزار

سخت‌افزار پایه‌ای‌ترین قسمت هر دستگاه متصل در IoT است. قطعات اصلی سخت‌افزار در حسگرها، پردازنده‌ها و ماژول‌های ارتباطاتی قرار دارند.

### ۳-۲-۱-۱-اینون‌سنس[۱۱۶]

این شرکت در زمینه حسگرهای مسیریابی MEMS و سیستم‌های میکروالکترومکانیکی، پیشرو است. ویژگی این قطعات، اندازه بسیار کوچک و مصرف توان کم آن‌هاست. بسیاری از این حسگرها، مانند ژیروسکوپ و شتاب‌سنج را می‌توان در گوشی‌های هوشمند امروزی یافت. حسگرهای MEMS با هدف IoT ساخته شده‌اند. با ایجاد میلیاردها دستگاه متصل در سال‌های آینده، رشد زیادی در حسگرهای MEMS اتفاق خواهد افتاد.

### ۳-۲-۱-۲-نوردیک ابررسانا[۱۱۷]

این شرکت نروژی، متخصص در زمینه تولید قطعات بی‌سیم با توان کم و وسایل ارتباطی برای باند ۲,۴گیگاهرتز که دارای توان مصرفی و هزینه پایین هستند، می‌باشد. تراشه‌های این شرکت در شمال اروپا به‌دلیل کیفیت و عملکرد خوبشان، به خصوص در کاربردهای بلوتوث، شناخته شده هستند. اگر فناوری آیبیکن[۱۱۸] که بر پایه بلوتوث است و توسط شرکت اپل مدیریت می‌شود، متوقف گردد، شرکت نوردیک در یک موقعیت عالی قرار خواهد گرفت.

### ۳-۲-۱-۳- شرکت کالمپ [۱۱۹]

این شرکت تولید کننده روتر، پورتال و سایر تجهیزات سخت‌افزاری در زمینه ارتباط M2M است. از زمانی که رویای صنعت اینترنت حقیقت یافت، شرکت کالمپ برای سودآوری از آن تأسیس شد. در ۳۰ سال گذشته این شرکت یک ارتباط ماشین به ماشین قانع کننده تولید کرده است.

---

[۱۱۶] InvenSense

[۱۱۷] Nordic Semiconductor

[۱۱۸] iBeacon

[۱۱۹] calAmp corp

### ۳-۲-۲- سهام‌های IoT در زمینه ارتباطات

وسایل متصل، داده‌هایی با حجم اگزابایت تولید می‌کنند. این داده‌ها نیاز به انتقال امن به گیرنده‌ها و یا پایگاه‌های داده دارند. به همین دلیل شرکت‌هایی در ایمن زمینه ایجاد شده است.

#### ۳-۲-۲-۱-جمالتو ان.وی.[۱۲۰]

یک شرکت امنیتی دیجیتال است که وظیفه ارائه برنامه‌های نرم‌افزاری کاربردی و دستگاه‌های شخصی امن را دارد. این شرکت هلندی در حال حاضر بر روی فضای مدیریت M2M کار می‌کند. جمالتو در زمینه ارائه یک ارتباط امن بین ماشین آلات و برنامه‌های کاربردی ابر، موقعیت بسیار خوبی دارد.

#### ۳-۲-۲-۲- سیرا بی‌سیم[۱۲۱]

این شرکت کانادایی متخصص در ارائه روش‌های ارتباط بی‌سیم سلولی در M2M است. سیرا بی‌سیم در حال حاضر صاحب ۳۴ درصد از بازار ماژول بی‌سیم M2M در سراسر جهان شده است. شرکت‌های تسلا و فورد ماژول‌های این شرکت را در اتومبیل‌های خود استفاده می‌کنند، و شهرهای لندن و پراگ نیز در روشنایی هوشمند از این ماژول‌ها بهره می‌برند.

### ۳-۲-۳- سهام‌های IoT در زمینه نرم‌افزارها/سیستم‌ها

تعدادی از دستگاه‌های متصل، از معماری نرم‌افزار/سیستم که در سال‌های اخیر در جریان "موج داده بزرگ" بوجود آمده، استفاده می‌کنند. اما این تنها بخشی از داستان است. برخی تحولات خاص در زمینه پردازش لحظه‌ای، ذخیره سازی و همچنین مدیریت دستگاه مرکزی ایجاد شده که نیاز به معماری نرم‌افزار/سیستم با استفاده از ابزارهای جدید را افزایش داده است.

---

[۱۲۰] Gemalto n.v.

[۱۲۱] Sierra wireless

### ۳-۲-۳-۱- PTC[۱۲۲]

PTC به عنوان یک شرکت نرم‌افزاری، در زمینه تولید نرم‌افزارهای طراحی دو بعدی و سه بعدی، مدیریت چرخه عمر محصول[۱۲۳] و راه‌حل‌های مدیریت خدمات شناخته می‌شود. در سال ۲۰۱۴، این شرکت وقتی دو پلتفرم برجسته IoT با نام‌های آکسدا[۱۲۴] و سینگورکس[۱۲۵] را ساخت، شناخته شد. این شرکت در تلاش برای ساختن یک نیروگاه برای IoT می‌باشد.

### ۳-۲-۳-۲- سافت‌ویر ای‌جی[۱۲۶]

تجزیه و تحلیل جریانی[۱۲۷] و یا لحظه‌ای، کلید اساسی در دسته‌بندی نوع تحلیل‌هایی است که در پردازش داده‌های IoT نیاز هستند. تحقیقات شرکت فورستر[۱۲۸]، به تازگی شرکت ای‌جی را به عنوان پیشرو در این زمینه قرار داده است. در حالی که سهم پیشرفت شرکت ای‌جی در بازار نرم‌افزار در حال کاهش است، این شرکت آینده خود را به عنوان یک سرمایه‌گذار در IoT می بیند.

### ۳-۲-۳-۳- لاگملن[۱۲۹]

یکی از رقبای بزرگ برای PTC در زمینه پلتفرم‌های IoT شرکت لاگملن است. محصول آن‌ها تحت عنوان ژیولی[۱۳۰] در رأس پلتفرم‌های IoT قرار دارد. اگر ژیولی، به عنوان پلتفرم IoT مسیر خود را ادامه دهد، می‌تواند تبدیل به

---

[۱۲۲] PTC

[۱۲۳] Product lifecycle management

[۱۲۴] Axeda

[۱۲۵] Thingworx

[۱۲۶] Software AG

[۱۲۷] Streaming

[۱۲۸] Forrester

[۱۲۹] LogMeln

[۱۳۰] xively

دروازه‌ای برای میلیاردها دستگاه متصل در سراسر جهان شود و با آن همه داده و مشخصه‌های اتصال، تقریباً مثل یک فیس‌بوک برای اشیاء عمل می‌کند.

### ۳-۲-۳-۴- انه‌آ[۱۳۱]

این شرکت سوئدی راه‌حل‌های سیستم عاملی، ازجمله ابزارهای توسعه، پروتکل‌های شبکه، پایگاه داده و میان افزار برای دستگاه‌های متصل ارائه می‌دهد. این شرکت ادعا می‌کند که سومین شرکت جهان در زمینه سیستم عامل‌های آنی[۱۳۲] است.

## ۳-۲-۴- سهام‌های IoT در حوزه کاربردهای تجارت

با تلاش شرکت‌هایی مانند جنرال الکتریک، اینترنت صنعتی سرعت بسیاری پیدا کرده است. شرکت‌های صنعتی در حال حاضر در حال افزایش محصولات و عملیات خود با استفاده از IoT هستند. علاوه بر این، برخی از شرکت‌ها به طور تخصصی در حال کمک به ساختن راه‌حل‌های صنعتی هستند.

### ۳-۲-۴-۱-فناوری‌های زبرا[۱۳۳]

در ابتدای سال ۲۰۱۴ زبرا، سرمایه‌گذاری شرکت موتورولا[۱۳۴] را برای تجارت تجهیزات به دست آورد. این شرکت به طور سنتی به عنوان یک شرکت پیشرو در زمینه بارکد و قطعات RFID است. زبرا در حال حاضر از تبدیل شدن به یک توانمندساز IoT در زمینه تجارت امتناع می‌کند. پلتفرم Zatar IoT، آخرین اقدام این شرکت در حوزه IoT است.

---

[۱۳۱] ENEA

[۱۳۲] Real-time

[۱۳۳] Zebra

[۱۳۴] Motorola

### ۳-۲-۴-۲- یوروتک[۱۳۵]

یک شرکت ایتالیایی کوچک است که دارای یک رویکرد ادغامی می‌باشد. این شرکت فناوری‌های ارتباطی و محاسباتی را در یک راه حل تجاری نوآورانه ادغام کرده است. یکی از پروژه‌های این شرکت توسعه حمل و نقل الکتریکی سریع و بدون سرنشین در فرودگاه هیترو[۱۳۶] در شهر لندن است.

## ۳-۲-۵- سهام IoT در حوزه برنامه‌های مصرف کننده

دوتا از بزرگترین بخش‌ها در زمینه برنامه‌های کاربردی مصرف کننده، در حال حاضر خانه‌های هوشمند و پوشیدنی‌ها هستند.

### ۳-۲-۵-۱-کنترل۴[۱۳۷]

در حوزه خانه هوشمند این شرکت بسیار جالب عمل می‌کند. در این شرکت محصولات برای خانه هوشمند (نظیر سوئیچر نور، کنترل دما و غیره) به گونه‌ای طراحی می‌شوند تا با دیگر محصولات در این زمینه هماهنگ باشند. در تقابل با عمده رقبای خود، این شرکت محصولات خود را بر پایه سخت‌افزار منبع باز و استانداردهای IP می‌سازد.

### ۳-۲-۵-۲- فناوری‌های لایف‌لاگر[۱۳۸]

این شرکت طراح دوربین‌های سبک‌وزن مجهز به حسگرها و موقعیت‌یاب‌های GPS است. لایف‌لاگر با وجود اینکه یک شرکت بسیار جوان است، اما در سال ۲۰۱۴ در میان ۵ شرکت دانش‌بنیان برتر قرار گرفت.

---

[۱۳۵] EuroTech

[۱۳۶] Heathrow

[۱۳۷] Control4

[۱۳۸] Lifelogger

### ۳-۲-۵-۳- ارو الکترونیک[۱۳۹]

ارو الکترونیک از سال ۱۹۳۰ متخصص در توزیع برق می‌باشد. امروزه این شرکت تأمین‌کننده تجهیزات اصلی بیش از صدهزار کارخانجات تولیدی در سراسر جهان است. ارو در زمینه IoT فعالانه تلاش می‌کند تا بتواند نقش خود را در ساخت میلیاردها وسیله متصل در آینده، ایفا کند. در دسامبر سال ۲۰۱۴ و اوایل سال ۲۰۱۵ کنفرانس " ارو و اینترنت اشیاء" در سه شهر ایالات متحده برگزار شد.

### ۳-۲-۵-۴- سیفگارد ساینتیفیک[۱۴۰]

این شرکت از معدود شرکت‌های سهامی عام است که به‌عنوان فراهم آورنده سرمایه برای شرکت‌های کارآفرین و دانش‌بنیان در حوزه IoT عمل می‌کند. سیفگارد در دسامبر سال ۲۰۱۳ یک پلتفرم تحت عنوان سینگ‌ورکس[۱۴۱] برای شرکت PTC طراحی کرده است.

در جدول ۳-۲-۵-۱ اطلاعات جامعی راجع به این شرکت‌ها آورده شده است.

**جدول ۳-۲-۵-۱ اطلاعات جامع از ۱۵ شرکت سهامی برتر در زمینه IoT**

| | شرکت | کشور | رده | زیررده | میزان تمرکز بر IoT | درآمد (M$) | رشد درآمدی |
|---|---|---|---|---|---|---|---|
| ۱ | زبرا تکنولوژی | آمریکا | کاربردهای تجاری | راه‌حل‌های صنعتی | ۲۵٪ | ۱۱۶۰ | ۶۱٪ |
| ۲ | سافت‌ویر ای.جی | آلمان | نرم‌افزار/سیستم | تحلیل جریانی | ۲۵٪ | ۱۰۹۰ | ۲٪ |
| ۳ | سیرا بی‌سیم | کانادا | مخابرات | خدمات M2M | ۱۰۰٪ | ۵۱۸ | |
| ۴ | سیفگارد ساینتیفیک | آمریکا | اکوسیستم گسترده‌تر | انصاف خصوصی[۱۴۲] | ۵۰٪ | | |

[۱۳۹] Arrow Electronics

[۱۴۰] Safeguard Scientifics

[۱۴۱] Thingworx

[۱۴۲] Private equity

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ۵ | پی.تی.سی | آمریکا | نرم‌افزار/ سیستم | پلتفرم IoT | ۲۵٪ | ۱۳۶۰ | ۳۱٪ |
| ۶ | نوردیک ابررسانا | نروژ | سخت‌افزار | پردازنده‌ها | ۱۰۰٪ | ۱۵۷ | ۳۹٪ |
| ۷ | لاگملن | آمریکا | نرم‌افزار/ سیستم | پلتفرم IoT | ۲۵٪ | ۲۰۷ | |
| ۸ | لایف‌لانگر | آمریکا | مصرف‌کننده | مصرف‌کننده | ۱۰۰٪ | ۰ | |
| ۹ | اینون‌سنس | آمریکا | سخت‌افزار | حسگرها | ۹۰٪ | ۲۸۲ | ۲۷٪ |
| ۱۰ | جمالتو | هلند | مخابرات | خدمات M2M | ۲۵٪ | ۲۹۵۰ | ۴۴٪ |
| ۱۱ | یوروتک | ایتالیا | کاربردهای تجاری | راه‌حل‌های صنعتی | ۱۰۰٪ | ۸۶ | |
| ۱۲ | انه‌آ | سوئد | نرم‌افزار/ سیستم | سیستم عامل | ۵۰٪ | ۵۵ | |
| ۱۳ | کنترل۴ | آمریکا | کاربردهای مصرف‌کننده | راه‌حل‌های مصرف‌کننده | ۱۰۰٪ | ۱۴۳ | ۶۰٪ |
| ۱۴ | کالمپ | آمریکا | سخت‌افزار | خدمات M2M | ۱۰۰٪ | ۲۴۱ | ۱٪ |
| ۱۵ | اروالکترونیک | آمریکا | اکوسیستم‌گسترده‌تر | خرده‌فروشی الکترونیکی | ۲۵٪ | ۲۲۵۳۰ | ۵۲٪ |

## ۳-۳- ۲۰ شرکت برتر در زمینه اینترنت اشیاء

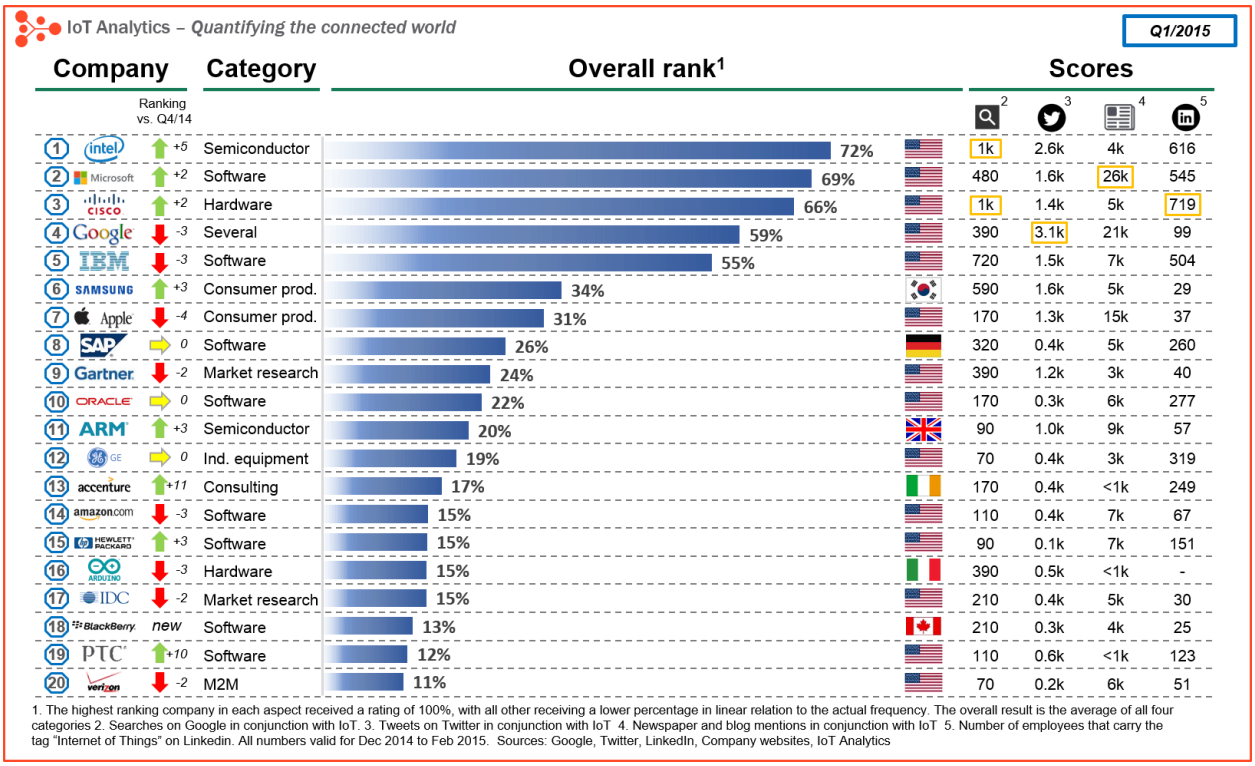
[http://iot-analytics.com/20-internet-of-things-companies/]

شرکت‌های فعال در زمینه اینترنت اشیاء توسط IoT Analytics از منظرهای گوناگون بررسی شده‌اند و ۲۰ شرکت برتر در این زمینه با توجه به معیارهای موجود، شناسایی شده‌اند. رتبه‌بندی این شرکت‌ها بر اساس پایگاه داده بیش از ۱۷۰۰ شرکت فعال در زمینه اینترنت اشیاء صورت پذیرفته است. همچنین در بررسی آن‌ها، چهار مسأله زیر نیز در نظر گرفته شده است:

- مردم معمولا درباره شرکت‌های مرتبط با اینترنت اشیاء چگونه در گوگل جست‌وجو می‌کنند.
- شرکت‌ها معمولا در رابطه با اینترنت اشیاء در توییتر چگونه مطرح می‌شوند.
- معمولا روزنامه‌ها و وبلاگ‌ها به شرکت‌های مرتبط با اینترنت اشیاء چگونه اشاره می‌کنند.

- چه تعداد از کارمندان شرکت‌ها در سایت Linkedin، برچسب اینترنت اشیاء دارند و در این حوزه کار می‌کنند.

بر اساس نتایج این تجزیه و تحلیل، یک رقابت تنگاتنگ بین ۵ شرکت اینتل[۱۴۳]، مایکروسافت[۱۴۴]، سیسکو[۱۴۵]، گوگل[۱۴۶] و IBM[۱۴۷] در زمینه اینترنت اشیاء وجود دارد. شکل ۳-۳-۱-۱، ترتیب کلی شرکت‌های پیشرو در زمینه IoT را به همراه حوزه کاری و اطلاعات آماری رتبه‌بندی، نشان می‌دهد:




**شکل ۳-۳-۱-۱رتبه‌بندی شرکت‌های دانش‌بنیان فعال در زمینه اینترنت اشیاء**

در ادامه به بررسی اجمالی این شرکت‌ها می‌پردازیم.

---

[۱۴۳] Intel

[۱۴۴] Microsoft

[۱۴۵] Cisco

[۱۴۶] Google

[۱۴۷] IBM

### ۳-۳-۱- اینتل

مدیر عامل شرکت اینتل، برایان کرانیچ[۱۴۸]، تجربه سختی در زمینه ایترنت اشیاء دارد. هنگامی که گوشی‌های هوشمند وارد بازار شدند، اینتل فکر نمی‌کرد که فرصت ارزشمندی در حال شکل گرفتن است. این شرکت زمانی به وسعت بازار گوشی‌های هوشمند پی برد که دیگر دیر شده بود و دیگران این فرصت را غنیمت شمرده بودند. حال در زمانی هستیم که اینترنت اشیاء وعده ۵۰ میلیارد وسیله متصل در ۵ سال آینده را می‌دهد، و کرانیچ با درسی که از گذشته آموخته این بار می‌خواهد از رقابت عقب نماند و مفهوم "اینتل در داخل[۱۴۹]" را در بین کارکنانش ترویج کند.

هم‌اکنون اینتل، پیش‌قدم در توسعه نسل جدید تراشه‌های کم مصرف[۱۵۰] برای دستگاه‌های متصل در اینترنت اشیاء شده است. آزمایشگاه‌های باز اینتل[۱۵۱] و تعدادی از همکاری‌های صنعتی، فشار فعالیت‌های شرکت اینتل در حوزه اینترنت اشیاء را به دوش می‌کشند. علاوه بر این هدف شرکت اینتل، تازه‌کارها و توسعه‌دهندگان نیز هست. در واقع کیت[۱۵۲] توسعه دهنده اینتل برای هرکس که می‌خواهد چیزی از خود تولید کند، به شدت در بازار سراسر جهان عرضه شده است. آخرین کار اینتل در حوزه اینترنت اشیاء را می‌توان طراحی یک پلتفرم جهت اتصال داده‌های تولید شده در اشیاء با فضای ابر دانست. در شکل ۳-۳-۱-۱ دیاگرام کلی این پلتفرم نمایش داده شده است.

---

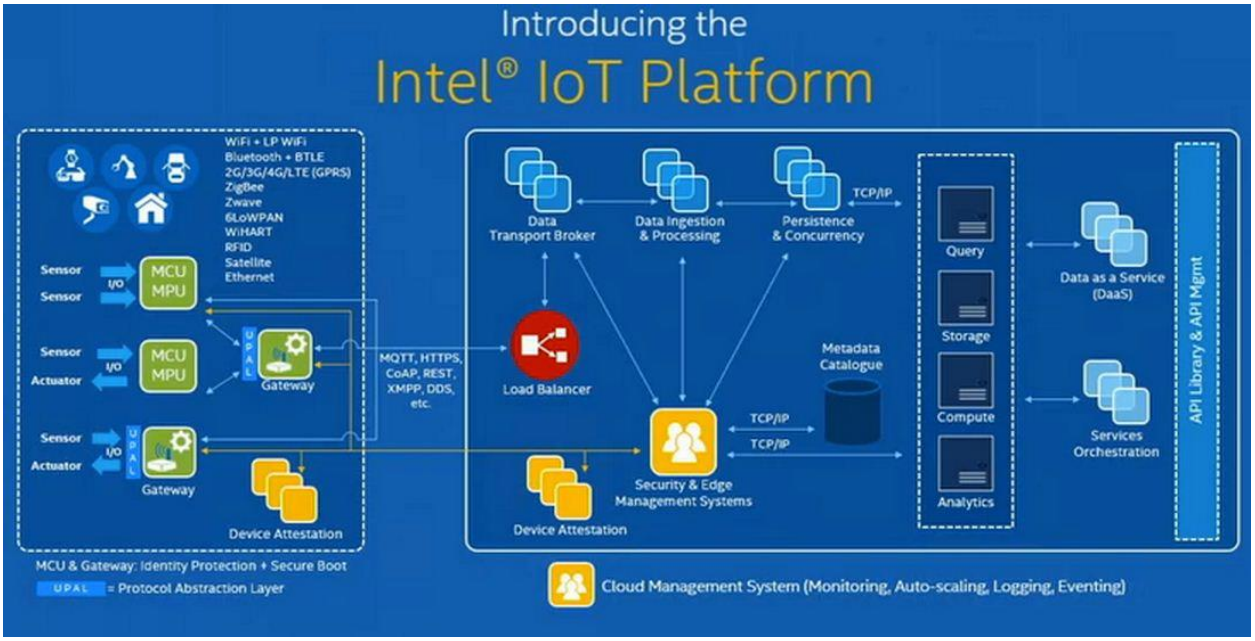
[۱۴۸] Brian Krzanich

[۱۴۹] Intel inside

[۱۵۰] Low-Power

[۱۵۱] Intel R&D centers

[۱۵۲] kit




**شکل ۳-۳-۱-۱دیاگرام پلتفرم اینتل برای اتصال به ابر[۱۵۳]**

## ۳-۳-۲- مایکروسافت

مایکروسافت نیز در زمینه گوشی‌های هوشمند به سرنوشتی مانند اینتل دچار شد. این شرکت با سهم ۳ درصدی در بازار سیستم عامل گوشی‌های هوشمند، رقابت در این بازار را از دست داده است.

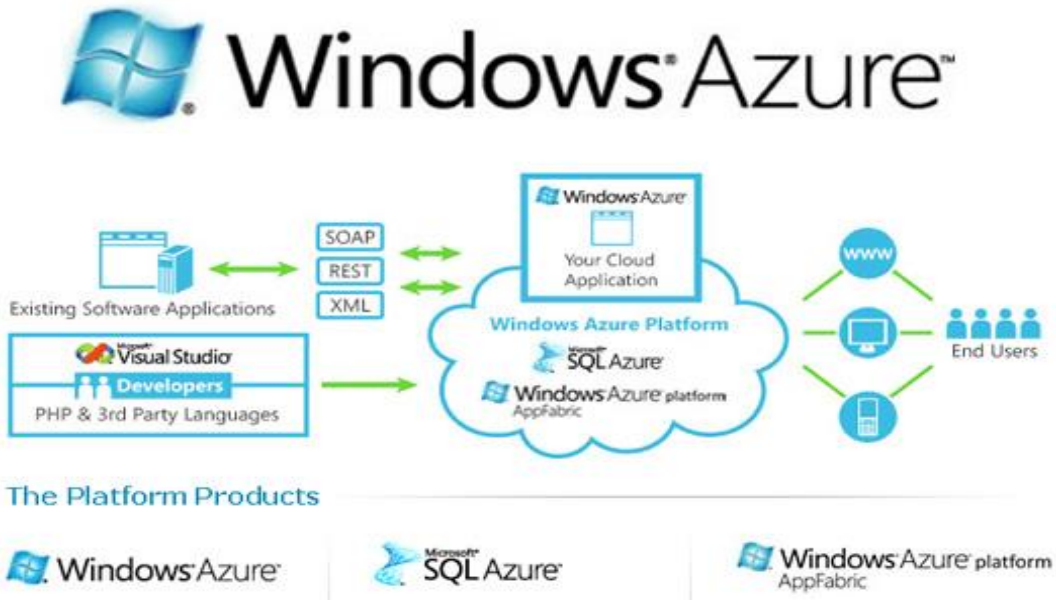
مایکروسافت در زمینه اینترنت اشیاء سه پیشنهاد ارائه می‌دهد: پیشنهاد اول، پلتفرم آزور[۱۵۴] است که انتظار می‌رود در آینده به یک پلتفرم فضای ابر[۱۵۵] برای اشیاء متصل تبدیل شود. پیشنهاد دوم تحلیل‌گرهای مایکروسافت هستند که برای پردازش لحظه‌ای داده‌های حاصل از حسگرها به کار می‌روند. پیشنهاد سوم این شرکت، پوشیدنی‌ها هستند که در حوزه سلامت و بهداشت مورد استفاده قرار می‌گیرند. در شکل ۳-۳-۲-۱ نحوه کاربری از پلتفرم آزور نشان داده شده است.

---

[۱۵۳] http://www.enterprisetech.com/2014/12/10/intel-rolls-iot-platform/

[۱۵۴] Azure

[۱۵۵] Cloud




شکل ۳-۳-۲-۱ پلتفرم آزور شرکت مایکروسافت

علاوه بر این تولیدات، این شرکت در حال بررسی و آزمایش در بخش صنعتی اینترنت اشیاء نیز هست. در پروژه‌ای مشترک با شرکت تولیدکننده ربات‌های هوشمند کوکا[۱۵۶]، مایکروسافت اخیرا موفق به ساخت یک ماشین بزرگی برای راه اندازی و مدیریت خطوط تولید کارخانجات شده است.

### ۳-۳-۳- سیسکو

"اینترنت برای همه" جمله‌ای است که اولین بار توسط شرکت سیسکو به کار برده شد. تأمین نیازهای سخت‌افزاری اینترنت اشیاء، حوزه اصلی فعالیت این شرکت در زمینه IoT است. در واقع باید گفت که سیسکو، با ساخت مسیریاب‌ها و سوییچ‌های شبکه، نیاز اساسی اینترنت اشیاء به ایجاد بستری مطمئن برای ارتباط را رفع می‌کند. علاوه بر ساخت ابزارهای شبکه، این شرکت راه‌حل‌هایی در حوزه امنیتی اینترنت اشیاء نیز ارائه داده است. سیسکو میزبان انجمن جهانی اینترنت اشیاء است. این شرکت با ارائه معماری پایان به پایان برای کارخانه‌ها توانسته است امکانات زیر را برای صنایع ایجاد کند:

۱- ادغام اتوماسیون صنعتی با سرعت و امنیت بیشتر و کنترل روش سیستم کسب و کار

[۱۵۶] Kuka

۲- ساخت یک شبکه مشترک، همگرا و نیرومند از کسب و کار

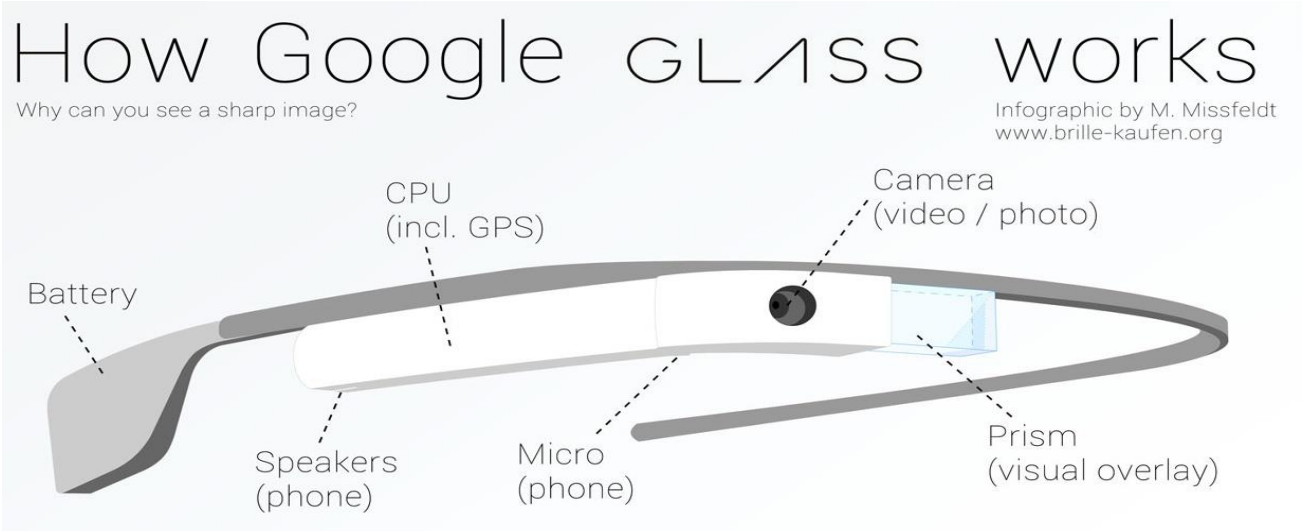
۳- بهبود هزینه‌های عملیاتی و بهره‌وری

۴- یافتن و رفع مشکلات در راه تولید ماکزیمم و در دسترس قرار دادن تجهیزات

۵- بهبود امنیت از طریق کنترل دسترسی کاربران به شبکه و تعیین هویت آن‌ها

### ۳-۳-۴- گوگل

گوگل روزانه در حال سرعت بخشیدن به تحقق اینترنت اشیاء است. در سال ۲۰۱۴ این شرکت، خرید کمپانی خانه هوشمند نست[۱۵۷] به ارزش ۳,۲ میلیارد دلار را تأیید کرد. عینک‌های هوشمند (شکل ۳-۳-۴-۱) و اتومبیل‌های بدون سرنشین، محبوب‌ترین پروژه‌های گوگل در زمینه اینترنت اشیاء هستند. اخیرا این شرکت اعلام کرده است که در حال ساخت یک پلتفرم برای زیرساخت فضای فیزیکی وب[۱۵۸] است، اما هنوز مشخص نیست که این پلتفرم، چه ویژگی‌هایی دارد. به هر حال حدس زده می‌شود که قرار است در زمینه اینترنت اشیاء، مورد استفاده قرار گیرد.




**شکل ۳-۳-۴-۱ ساز و کار عینک هوشمند گوگل**

[۱۵۷] Nest

[۱۵۸] Physical web

### ۳-۳-۵- IBM

IBM طیف گسترده‌ای از خدمات و فناوری‌های به روز را ارائه می‌دهد که از مهم‌ترین آن‌ها، توسعه نرم‌افزارها و سیستم‌های مدیریت سرورها و ابر رایانه‌های جهان است. اما در زمینه IoT این شرکت از ابزاری به نام بنیاد اینترنت اشیاء[۱۵۹] استفاده می‌کند. این ابزار، نوعی از توانایی را در سیستم ایجاد می‌کند که قابلیت ورود دستگاه جدید به مجموعه وجود داشته باشد، و همچنین امکان کنترل و ذخیره‌سازی داده‌های به دست آمده از IoT میسر باشد. سرویس مذکور توانایی‌های بنیادینی برای ساخت صنایع دارد که از جمله آن‌ها می‌توان به موارد زیر اشاره کرد:

۱- اتصال: به راحتی هر چیزی را می‌توان معرفی و متصل کرد.

۲- جمع‌آوری: جمع‌آوری و مدیریت مشخصات داده‌ها در هر زمان و از همه چیز

۳- مونتاژ: اتفاقات و رویدادها را به صورت گرافیکی از IoT به زبان منطقی تبدیل می‌کند

۴- مدیریت: مدیریت ارتباطات و اشتراک با یک سرویس بسیار مقیاس پذیر

### ۳-۳-۶- سامسونگ

سامسونگ یکی از بزرگترین شرکت‌های تولید کننده گوشی‌های هوشمند، اشیاء پوشیدنی، تلویزیون‌های هوشمند، چاپگرها و لوازم خانگی است. این شرکت علاقه‌مندی زیادی به اینترنت اشیاء دارد. اخیرا سامسونگ پروتکل خانه هوشمند[۱۶۰] را ارائه داده که امکان اتصال همه وسایل خانگی را فراهم می‌کند. با استفاده از این پروتکل می‌توان ماشین لباسشویی، تهویه کننده، لامپ‌ها و غیره را از بیرون منزل و تن‌ها با یک گوشی هوشمند مدیریت کرد (شکل ۳-۳-۶-۱).

[۱۵۹] Internet of Things foundation

[۱۶۰] Smart Home Protocol (SHP)


شکل ۳-۳-۶-۱ مدیریت وسایل خانه با استفاده از گوشی‌های هوشمند

### ۳-۳-۷- اپل[۱۶۱]

کار اپل روی IoT همانند کارهای قبلی این شرکت بزرگ، بیشتر به طور مخفی صورت می‌گیرد. در پشت پرده پیشرفت‌هایی رخ می‌دهد و سپس با صدای بلند آن‌ها را مطرح می‌کند. در حال حاضر فعالیت‌های این شرکت در زمینه IoT بر روی ساعت اپل و پلتفرم هوم‌کیت[۱۶۲] متمرکز شده است. در واقع هنوز معلوم نیست که قرار است در آینده اپل با چه وسیله‌ای ما را شگفت‌زده کند، اما واضح است که این شرکت بزرگ برای همه زمینه‌های IoT برنامه‌هایی دارد. هرچند خود این شرکت هنوز تأیید نکرده، اما شواهدی مبنی بر این وجود دارد که اپل قصد دارد به بازار تجارت اتومبیل‌های متصل، وارد شود.

### ۳-۳-۸- سَپ[۱۶۳]

شرکت آلمانی سپ، یکی از بزرگترین سرمایه‌گذاران در زمینه تجارت نرم‌افزار است. این شرکت اعتقاد دارد که با ظهور IoT بازار نرم‌افزار به کلی متحول خواهد شد. سپ در تلاش است تا پایگاه داده هانا[۱۶۴] را به نحوی تثبیت کند

---

[۱۶۱] Apple

[۱۶۲] HomeKit

[۱۶۳] SAP

[۱۶۴] HANA

که در آینده با استفاده از این پایگاه داده، امکان ایجاد بستری برای فضای ابر به سهولت امکان‌پذیر باشد. این شرکت علاوه بر این که سیستم ERP[۱۶۵] خود را با IoT هماهنگ و آن را با پلتفرم M2M، آزمایش کرده است، پروژه‌هایی در زمینه‌های ساخت، سرویس‌دهی و تدارکات نیز انجام داده است.

### ۳-۳-۹- گارتنر[۱۶۶]

گارتنر یک شرکت راهنما و تحقیقاتی در زمینه اتفاقات دنیای فناوری اطلاعات است. در واقع این شرکت داده‌های مربوط به زمینه‌های مرتبط با فناوری اطلاعات را جمع‌آوری می‌کند، و آن‌ها را در اختیار کاربران خود قرار می‌دهد، تا بتوانند تصمیم درست را اتخاذ کنند.

این شرکت در زمینه IoT، بیشتر به خاطر نمودار چرخه هایپ[۱۶۷] خود مشهور است. در سال ۲۰۱۱ گارتنر نموداری در ارتباط با فناوری‌های نوظهور منتشر کرد که اینترنت اشیاء، در قسمت صعودی این نمودار قرار داشت. گارتنر در سال ۲۰۱۴ اعلام کرد که بالاخره اینترنت اشیاء توانست به قله این نمودار برسد. الان دیگر زمان آن رسیده که در مسیر نزولی نمودار قرار گیرد؛ اما خیلی از شرکت‌هایی که در زمینه اینترنت اشیاء فعالند، امیدوارند برای یک بار هم که شده پیش‌بینی‌های این شرکت درست نباشد.

### ۳-۳-۱۰- اراکل[۱۶۸]

عمده کار این شرکت، توسعه، تولید و پشتیبانی از پایگاه‌های داده و میان‌افزارها[۱۶۹]، نرم‌افزارهای کاربردی، زیرساخت‌های فضای ابری، سیستم‌های سخت افزاری و سایر خدمات مرتبط در سرتاسر جهان است.

---

[۱۶۵] ERP

[۱۶۶] Gartner

[۱۶۷] Hype-circle

[۱۶۸] Oracle

[۱۶۹] Middleware

این شرکت در زمینه فناوری IoT و توسعه آن تحقیقات بسیاری انجام داده است که از جمله مهمترین آن‌ها می‌توان به تولید میان‌افزارهای مناسب و نیز ارائه یک چارچوب کلی برای معماری این فناوری اشاره کرد. چارچوب طراحی شده توسط شرکت اراکل، یک ساختار یکپارچه، امن و جامع برای معماری IoT در تمام حوزه‌ها ارائه می‌کند. این چارچوب دارای مزایای زیر است:

۱- توانایی دریافت و ارسال پاسخ در هر لحظه میان میلیون‌ها وسیله مرتبط در این فناوری

۲- زمان سریع‌تر برای داد و ستد کالا

۳- برقراری امنیت

۴- قابلیت ادغام با سیستم‌های IT

۵- ایجاد یک اکوسیستم جهانی از همکاران

۶- قابلیت پایان به پایان[۱۷۰] و مدیریت چرخه عمر

### ۳-۳-۱۱- آرم[۱۷۱]

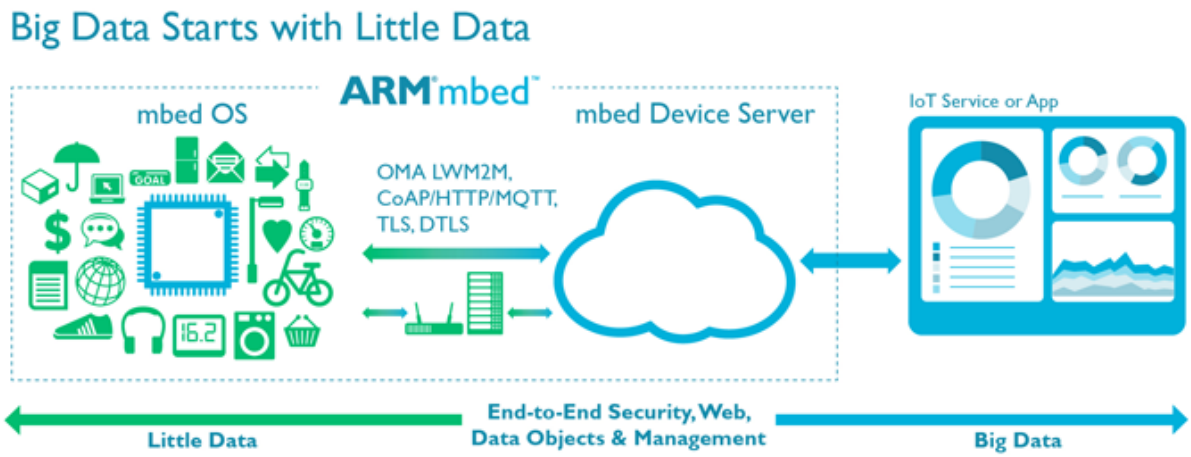
این شرکت تولید کننده حسگرها، کنترل کننده‌ها و سایر قطعات هوشمند جاسازی شده در اشیاء است. وسعت عملکرد فناوری‌های آرم شامل IP سیلیکون و ابزارها و نرم افزارهای IP با رویکردی مشارکتی، نیازهای درحال تکامل امنیت ارتباطات در IoT را پاسخ می‌دهد و سریع‌ترین و کارامدترین راه برای استقرار سیستم عامل و سایر خدمات را فراهم می‌کند.

پلتفرم ARMmbed سریع‌ترین راه برای ایجاد سازگاری بین اجزای IoT و برپایه میکرو کنترل‌های آرم است. این طرح مجموعه‌ای از استانداردهای باز که بر پایه طرح‌های متداول هستند را ارائه می‌کند و همچنین یک اکوسیستم جدید برای IoT ارائه می‌دهد که در آن رابطه بین دستگاه‌ها و ابر برقرار شده است (شکل ۳-۳-۱۱-۱).

---

[۱۷۰] End-to-End

[۱۷۱] ARM




شکل ۳-۳-۱۱-۱ پلتفرم آرم

طرح مذکور دارای مزایای زیر است:

۱- حل مشکل تکه تکه شدن معماری با ارائه یک سیستم عامل پایه برای دستگاه‌های IoT

۲- به کار انداختن طرح‌های آینده به وسیله حمایت از استانداردهای ارتباط و مدیریت اشیاء

۳- فعال کردن وسایل امن و قابل به روز رسانی که قادر به پردازش و عملکردهای بسیاری هستند

۴- حل مشکل مصرف انرژی به وسیله مدیریت قدرت به طور اتوماتیک

۵- ایجاد ابر مبتنی بر توسعه ابزارها به نحوی که شما محصولات خود را سریع‌تر از همیشه توسعه دهید.

### ۳-۳-۱۲- جنرال الکتریک[۱۷۲]

جنرال الکتریک یک شرکت چند ملیتی در آمریکا است که عمده فعالیت‌های آن از سال ۲۰۱۵ در زمینه‌های آب و برق، نفت و گاز، مدیریت انرژی، هوانوردی، حمل و نقل، بهداشت سلامت و سرمایه است.

این شرکت در میان شرکت‌های پیشرو در زمینه صنعت IoT است. جنرال الکتریک در برخی از صنایع همچون حمل و نقل هوایی، تولید و مصرف برق راهکارهایی برای استفاده از اینترنت اشیاء ارائه می‌دهد. این شرکت ادعا می‌کند که با محصولات اینترنت صنعتی خود در سال ۲۰۱۴ به درامدی بالغ بر یک میلیارد دلار دست یافته است.

[۱۷۲] General Electric

### ۳-۳-۱۳-اکسنچر[۱۷۳]

اکسنچر یک شرکت ایرلندی است که عمده فعالیت‌های آن در زمینه مشاوره مدیریتی و خدمات فناوری است. در واقع این شرکت، به سازمان‌هایی که تحت نظارتش قرار دارند، کمک می‌کند که وضعیتشان را بهبود بخشند.

در زمینه IoT، با توجه به داده‌های آماری که این شرکت به دست آورده است، کاربرانش را ترغیب به بهره‌برداری از این فناوری می‌کند. به خصوص این‌که عمده تمرکز این شرکت در بحث صنعت اینترنت اشیاء است.

### ۳-۳-۱۴- آمازون[۱۷۴]

این شرکت که بیشتر به عنوان یک فروشگاه اینترتی در سراسر جهان معروف است، سازنده یک وسیله هوشمند به نام اکو[۱۷۵] است، با این قابلیت که می‌تواند براساس صدایی که به آن فرمان می‌دهد، موسیقی دلخواه را اجرا کند. انتظار می‌رود در آینده این وسیله به عنوان یک همدم خانگی که به اینترنت وصل است، عمل کند (شکل ۳-۳-۱۴-۱).

آمازون در زمینه IoT در حال توسعه فضای ابری است که در آن اشیاء به راحتی بتوانند متصل شوند.


[۱۷۳] Accenture

[۱۷۴] Amazon

[۱۷۵] Echo

شکل ۳-۳-۱۴-۱اکو آمازون

### ۳-۳-۱۵-HP[۱۷۶]

یک شرکت آمریکایی است که به مشتریان خود خدمات سخت‌افزاری/نرم‌افزاری ارائه می‌دهد. HP مطابق با رسالت خود در دنیای دیجیتال، در زمینه IoT نیز اقداماتی انجام داده است. شاید بتوان گفت طراحی و پیاده‌سازی پلتفرم هلیون[۱۷۷] که یک پلتفرم منبع باز[۱۷۸] برای فضای ابر است، شاخص‌ترین کار HP در زمینه اینترنت اشیاء باشد. ویژگی منبع باز بودن این امکان را فراهم می‌کند، که بتوان به فراخور نیاز آن را برای کاربری وسایل متصل برنامه‌ریزی کرد.

### ۳-۳-۱۶- آردوینو[۱۷۹]

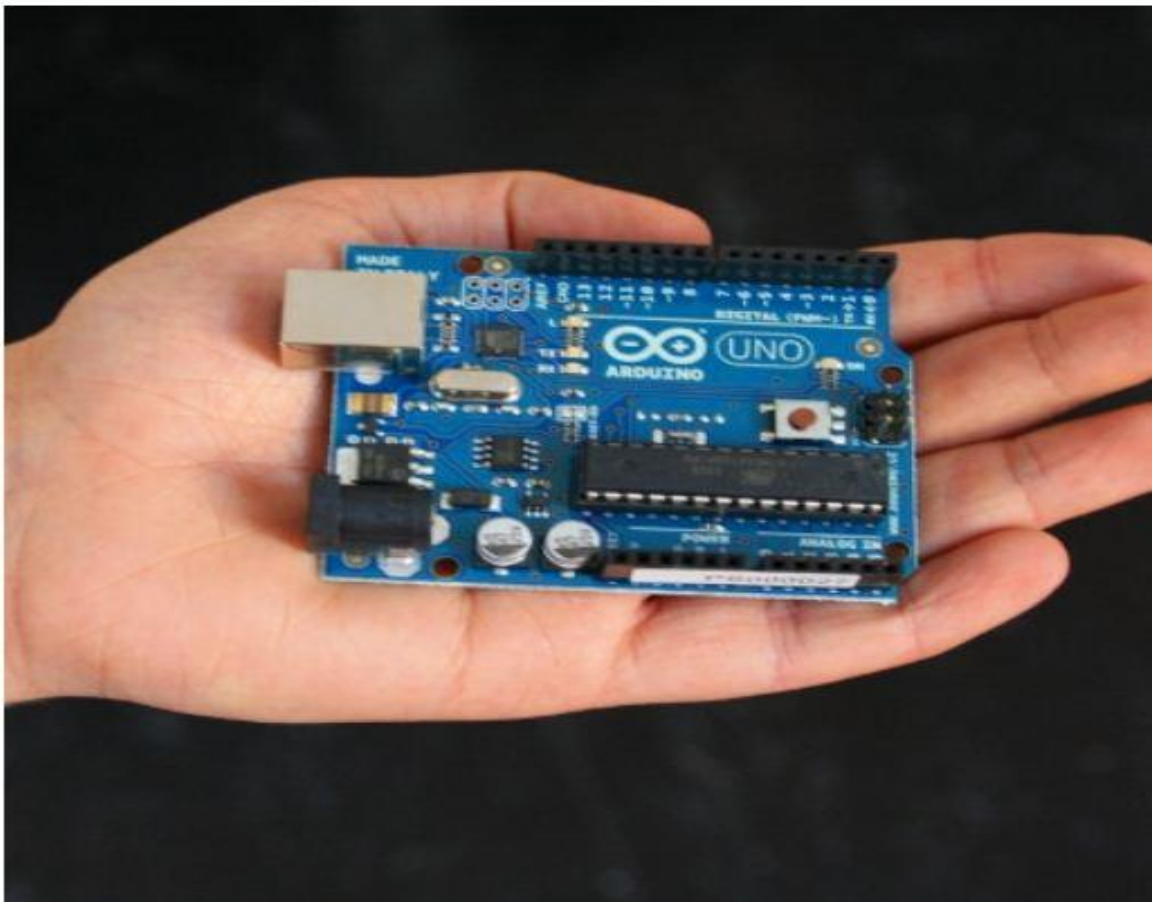
یک شرکت کامپیوتری منبع باز، در زمینه سخت‌افزار و نرم‌افزار است. این شرکت، کیت‌هایی برای وسایل دیجیتال و اشیاء ارتباطی که می‌توانند دنیای فیزیکی را حس و کنترل کنند؛ طراحی و تولید می‌کند. در واقع این شرکت بردهایی طراحی می‌کند که در ساختار قطعات دیگر به کار می‌روند. در واقع آردوینو یک قطعه کوچک و ارزان است که به شما این امکان را می‌دهد، تا به راحتی برخی از اشیاء الکترونیکی خود را به رایانه و در نهایت به اینترنت وصل کنید (شکل ۳-۳-۱۶-۱).

[۱۷۶] HP

[۱۷۷] Helion

[۱۷۸] Open-source

[۱۷۹] Arduino




شکل ۳-۳-۱۶-۱ بردهای آردوینو

### ۳-۳-۱۷-IDC[۱۸۰]

این شرکت، مشابه گارتنر، در زمینه‌های بازار و تجارت فناوری‌های دیجیتال تحقیق می‌کند. حوزه‌های تحقیقاتی این شرکت فناوری اطلاعات، مخابرات و فناوری‌های مصرفی است. با تحقیقاتی که این شرکت در سال ۲۰۱۳ و ۲۰۱۴ انجام داد، لیستی جامع از زمینه‌هایی که با ظهور اینترنت اشیاء متحول خواهند شد منتشر کرده است. این لیست توسط این شرکت به قیمت چند هزار دلار به فروش رفت.

[۱۸۰] IDC

### ۳-۳-۱۸-بلک‌بری[۱۸۱]

یک شرکت کانادایی تولید کننده قطعات مخابرات و اتصالات بی‌سیم است که در بین عوام، بیشتر به دلیل گوشی‌های هوشمند و تبلت‌هایش شهرت دارد. این شرکت در سراسر جهان به عنوان یکی از تولید کنندگان نرم‌افزارهای امن و مطمئن برای صنایع مختلف شناخته می‌شود.

پلتفرم IoT بلک‌بری، مجموعه‌ای کامل از اجزایی است که شامل نرم‌افزار اشیاء، خدمات ابر و رابط داده است. پلتفرم خدمات ابر این شرکت دارای ۳ هسته اصلی است:

۱- بنیاد پلتفرم[۱۸۲]با پیام‌دهی مرکزی

۲- منطق تجارت برای ایجاد کاربری‌های ویژه

۳- ماژول کاربرد برای ارتباط با توسیع‌دهندگان

در ادامه هر کدام از عناوین فوق را توصیف می‌کنیم.

بنیاد پلتفرم IoT بلک‌بری، بسیار قابل اطمینان و با سیستم پیام‌دهی مقیاس‌پذیر است که برای نمایش و ذخیره به کار می‌رود. این بخش دارای عملکرد پاسخ‌گو و تبادل اطلاعات امن است که به عنوان گذرگاه پیام طراحی شده است.

منطق تجارت بخشی است که در آن اطلاعات از اشیاء با ابزارهای IoT درک و تحلیل می‌شود.

بسته کاربرد، یک ابزار با طراحی از قبل یکپارچه[۱۸۳] در اختیار قرار می‌دهد تا بتوان پیاده سازی راهکارهای IoT را ساده‌تر و عملی‌تر کرد.

### ۳-۳-۱۹-PTC

یک شرکت نرم‌افزاری آمریکایی است که متخصص در طراحی نرم‌افزارهای طراحی دو بعدی و سه بعدی، مدیریت چرخه عمر محصولات و راهکارهای مدیریت خدمات رسانی است. در زمینه IoT این شرکت دارای دو محصول بسیار

---

[۱۸۱] Blackberry

[۱۸۲] Platform Foundation

[۱۸۳] Pre-integrated

معروف است. یکی پلتفرم سینگ‌ورکس[۱۸۴] است که برای توسعه سریع کاربردهایی که برای جهان هوشمند (حسگرها و ابزارها و تولیدات IoT) ساخته شده‌اند ، به کار می‌رود. دیگری آکسدا[۱۸۵] است که یک نرم‌افزار خدمت‌رسانی ابر-مبنا، برای مدیریت تولیدات و ماشین‌های متصل و همچنین اجرای نوآورانه کاربردهای IoT است.

### ۳-۳-۲۰-وریزون[۱۸۶]

وریزون یکی از شرکت‌های پیشتاز در زمینه، خدمات مدیریت شده ماشین-به-ماشین[۱۸۷] در شمال آمریکا است. این فناوری اجازه می‌دهد تا ارتباط داده از طریق شبکه سلولار فراهم شود. وریزون همچنین نمایشگاه‌هایی در سراسر دنیا از راهکارهای مخابراتی، برای بهداشت و سلامت متصل و فناوری‌های اتومبیل متصل برگزار می‌کند.

## ۳-۴- دانشگاه‌ها

اساس و بنیان هر فناوری، مطالعات و تحقیقات نظری می‌باشد که قبل از آن‌که آن فناوری پا به عرصه حضور نهد، انجام شده است. در واقع این مطالعات نظری هستند که می‌توانند باعث پیشرفت و ایجاد هر فناوری گردند. اینترنت اشیاء نیز به عنوان یک فناوری نوظهور، نیاز به مطالعات نظری گسترده در حوزه‌های مختلف آن، از پایه ریزی زیرساخت، تا مباحث پیاده سازی عملی و امنیت، دارد.

بدون شک دانشگاه‌ها به عنوان مراکز تحقیقاتی هر جامعه‌ای، بنیادی‌ترین مکان برای انجام پژوهش‌های نظری می‌باشند. هر فناوری که امروزه مورد استفاده عملی قرار می‌گیرد، طرح و ایده‌اش به صورت نظری، ابتدا به ساکن در محیط‌های آکادمیک مطرح شده است. این دانشگاه است که با پرورش نیروهای محقق جوان، زمینه‌های نوآوری و پتانسیل حل مسائل پیچیده را در آن‌ها ایجاد می‌کند تا بتوانند به سطح بالایی از دانش، برای رفع نیازهای اساسی هر فناوری، دست یابند.

---

[۱۸۴] ThingWorx

[۱۸۵] Axeda

[۱۸۶] Verizon

[۱۸۷] M2M

با توجه به این مطالب، در این بخش چند دانشگاه بزرگ دنیا و پروژه‌هایشان در زمینه IoT را بررسی می‌کنیم.

### ۳-۴-۱- دانشگاه استنفورد[۱۸۸]

[http://internet-of-things.meetup.com/cities/us/ca/stanford/]

[http://dataconomy.com/stanford-researchers-invent-multistoried-chips-to-address-the-rise-of-iot-and-big-data/]

[http://iot.stanford.edu/people.html]

[http://www.technologyreview.com/news/534506/sniffing-radio-frequency-emissions-to-secure-the-internet-of-things/]

دانشگاه استنفورد یکی از معتبرترین دانشگاه‌های دنیا است که در استنفورد، در نزدیکی شهر سانفرانسیسکو[۱۸۹] در ایالت کالیفرنیا[۱۹۰] در کشور آمریکا قرار دارد. دانشکده‌های این دانشگاه عبارتند از: علوم، بازرگانی، حقوق، پزشکی و مهندسی. این دانشگاه در سال ۱۸۸۵ به دست لیلند استنفورد[۱۹۱] و همسرش ساخته شد. جمعیت دانشجویان استنفورد در حدود ۷۰۰۰ نفر دانشجوی دوره‌های مقدماتی ثبت نام شده و حدود ۹۰۰۰ دانشجوی تحصیلات تکمیلی از ایالات متحده و سایر نقاط جهان می‌باشد. دانشگاه استنفورد در منطقه دره سیلیکون[۱۹۲] در ایالت کالیفرنیا واقع است و بسیاری از شرکت‌های معتبر در زمینه فناوری اطلاعات توسط فارغ‌التحصیلان این دانشگاه تأسیس شده‌اند. از

[۱۸۸] Stanford

[۱۸۹] San Francisco

[۱۹۰] California

[۱۹۱] Amasa Leland Stanford

[۱۹۲] Silicon

مشهورترین این شرکت‌ها می‌توان به سان مایکروسیستمز[۱۹۳]، هیولت پاکارد[۱۹۴]، یاهو[۱۹۵]، گوگل[۱۹۶]، الکترونیک آرتز[۱۹۷] و سیسکو[۱۹۸] اشاره کرد.

اینترنت به زودی ما را به جهان فیزیکی، از طریق شبکه‌ی حسگرها، خانه‌های هوشمند، اتومبیل‌های هوشمند و شبکه‌های خودکار پیوند خواهد زد. این کاربری گسترده با چالش‌ها و خطرات امنیتی بسیاری همراه است. اگر امروزه هکرها به دنبال دزدیدن اطلاعات کارت اعتباری افراد هستند، در آینده و با ظهور اینترنت اشیاء، این اطلاعات منزل، سلامت و یا دنبال کردن مسیرهای رفت و آمد افراد است که برایشان ارزشمند خواهد بود. پروژه اینترنت اشیاء امن[۱۹۹](SITP)، یک پروژه ۵ ساله است که در دانشگاه استنفورد و با همکاری این دانشگاه و دو دانشگاه برکلی[۲۰۰] و میشیگان[۲۰۱]، با هدف پژوهش اساسی، در جهت یافتن راه‌های بهینه در افزایش امنیت سیستم‌های مبتنی بر اینترنت اشیاء، در حال انجام است. این پژوهش در تلاش است تا به سه سوال زیر پاسخ دهد:

۱- تحلیل: چگونه می‌توانیم این حجم از اطلاعات؛ از ابزارهای فیزیکی اطرافمان را با داده‌های موجود تطبیق دهیم تا تداخلی ایجاد نشود؟

۲- امنیت: چگونه می‌توان سیستم‌های حسگری و تحلیلی را از دستبرد اطلاعات، مصون داشت؟

۳- سیستم‌های سخت‌افزاری و نرم‌افزاری: کدام سیستم سخت‌افزاری و نرم‌افزاری، به ما کمک می‌کند تا بتوانیم، کاربری اینترنت اشیاء هوشمند و امن را به راحتی کاربری وب ایجاد کنیم؟

---

[۱۹۳] Sun Microsystems

[۱۹۴] Hewlett-Packard

[۱۹۵] Yahoo

[۱۹۶] Google

[۱۹۷] Electronic Arts

[۱۹۸] Cisco

[۱۹۹] Secure Internet of Things Project

[۲۰۰] Berkeley

[۲۰۱] Michigan

دانشگاه استنفورد با داشتن یکی از قویترین دانشکده‌های علوم کامپیوتر و برق در دنیا، و با تکیه بر تیم قوی رمزنگاری‌اش در تلاش است تا بتواند به این چالش‌های پیش‌رو پاسخی جامع و کارا دهد.

### ۳-۴-۲- دانشگاه برایتون[۲۰۲]

[http://en.wikipedia.org/wiki/University_of_Brighton]
[http://www.digitalcatapultcentre.org.uk/local-centre/brighton/]

این دانشگاه، یک دانشگاه انگلیسی با حدود ۲۱ هزار دانشجو است. تعداد دانشکده‌های این دانشگاه ۵ تا است که عبارتند از: دانشکده هنر، دانشکده تربیت بدنی، دانشکده سلامت و علوم اجتماعی، دانشکده علوم و مهندسی و دانشکده پزشکی.

دانشگاه‌ها همواره با گرفتن طرح‌های پژوهشی از صنعت و تعریف پایان‌نامه‌های تحصیلات تکمیلی بر اساس این طرح‌ها، برای خود و دانشجویانشان فرصت شغلی ایجاد می‌کنند. دانشگاه برایتون نیز با تعریف صدها پروژه در زمینه اینترنت اشیاء، و ترغیب دانشجویان به انجام تحقیقات در این زمینه، به پیشبرد و عملی کردن اینترنت اشیاء کمک می‌کند، از طرح‌های تحقیقاتی در زمینه اینترنت اشیاء که در این دانشگاه در حال انجام است می‌توان طرح‌ها و رساله‌های زیر را نام برد:

مخابرات ناهمگون و محاسبات ابری در اینترنت اشیاء به سرپرستی پرفسور شنگ[۲۰۳]، عملیات کم-توان در انجام محاسبات و الکترونیک پوشیدنی‌های هوشمند تحت نظارت دکتر راگن[۲۰۴]، امنیت پویا برای IoT تحت سرپرستی پروفسور موراتیدیس[۲۰۵].

---

[۲۰۲] Brighton

[۲۰۳] Sheng

[۲۰۴] Roggen

[۲۰۵] mouratidis

این دانشگاه همچنین دارای یک آزمایشگاه بزرگ تحت عنوان مرکز منجنیق دیجیتال[۲۰۶] می‌باشد، که مشخصا روی پروژه‌هایی در زمینه تحلیل لحظه‌ای مکان با استفاده از داده‌های دریافتی از اشیاء، تحت عنوان اینترنت مکان[۲۰۷] کار می‌کند.

### ۳-۴-۳- دانشگاه ETH زوریخ[۲۰۸]

انستیتو تکنولوژی فدرال زوریخ، یکی از دانشگاه‌های مهم کشور سوئیس است که مرکز آن در شهر زوریخ قرار گرفته است. این دانشگاه همچنین در فهرست «برترین دانشگاه‌های جهان» که توسط مؤسسه اروپایی تحقیقات دانشگاهی انجام شد، در رده ۱۳ جهان قرار دارد. درحال حاضر بیش از ۱۷۰۰۰ دانشجو از ۸۰ کشور جهان در مقاطع مختلف مشغول تحصیل هستند. این دانشگاه ۳۰ برنده جایزه نوبل را در لوح افتخارات خود دارد. رشته‌های تحصیلی دانشگاه عبارتند از: مهندسی مکانیک، مهندسی عمران، معماری، شیمی، جنگل‌داری، ریاضیات و علم سیاست.

دانشگاه ETH در زمینه IoT دو طرح تحقیقاتی بزرگ را انجام داده است. طرح تحقیقاتی اول که با همکاری گروه سیستم‌های توزیع شده[۲۰۹] می‌باشد، طراحی یک پلتفرم نرم‌افزاری RFID، منبع-باز است که تحت عنوان فوستراک[۲۱۰] شناخته می‌شود. این پلتفرم استفاده از RFIDها را آسان‌تر و کارایی آن‌ها را افزایش می‌دهد. طرح تحقیقاتی بعدی، تحت عنوان منابع وب جاسازی شده[۲۱۱] شناخته می‌شود. این پروژه اختصاص به طراحی یک لایه کاربرد وب-مانند، برای بسیاری از ابزارهای منبع محدود دارد. این پروژه برنامه‌ریزی برای کاربردهای اینترنت اشیاء را آسان‌تر کرده است.

---

[۲۰۶] Digital Catapult Centre

[۲۰۷] Internet of place

[۲۰۸] Zürich

[۲۰۹] Distributed systems group

[۲۱۰] fosstrak

[۲۱۱] Embedded Web Resources

### ۳-۴-۴- دانشگاه مالمو[۲۱۲]

[http://en.wikipedia.org/wiki/Malm%C3%B6_University]

دانشگاه مالمو در سال ۱۹۹۸ و در شهر مالمو کشور سوئد تأسیس شد. این دانشگاه با حدود ۲۴۰۰۰ دانشجو، به عنوان نهمین مرکز تحقیقاتی-آموزشی در سوئد شناخته می‌شود. دانشکده‌های این دانشگاه عبارتند از: دانشکده تکنولوژی و جامعه، دانشکده فرهنگ و جامعه، دانشکده تحصیل و جامعه، دانشکده دندانپزشکی و دانشکده سلامت و جامعه. یکی از مراکز تحقیقاتی بزرگ در این دانشگاه، مرکز تحقیقاتی IoT می‌باشد.

این دانشگاه دارای یک مرکز تحقیقاتی، تحت عنوان اینترنت اشیاء و افراد[۲۱۳] است که بر روی نحوه پذیرش تولیدات اینترنت اشیاء توسط افراد جامعه تحقیق می‌کند. این تحقیق شامل دانشمندان، طراحان و کاربران علوم کامپیوتر می‌شود. در واقع این مرکز تحقیقاتی بر روی عناوین زیر تمرکز دارد:

- چگونه کاربران با اشیاء متصل روبرو می‌شوند.
- چگونه افراد در خدمات و تولیدات جدید IoT می‌توانند درگیر شوند.
- چگونه هوشمندی که در داخل اشیاء قرار داده شده است، می‌تواند پایداری و کارآیی خدمات و تولیدات IoT را بهبود بخشد.

### ۳-۴-۵- دانشگاه جورجیا تک[۲۱۴]

مؤسسه فناوری جورجیا که اغلب از آن با نام جورجیا تک یاد می‌شود، دانشگاهی پژوهش‌محور و دولتی واقع در آتلانتا در ایالت جورجیای آمریکا است. این دانشگاه یکی از بخش‌های سیستم دانشگاهی ایالت جورجیا به شمار می‌رود و دارای واحدهایی اقماری در شهرهای ساوانای جورجیا، متز فرانسه، اتلون ایرلند، شانگهای چین و سنگاپور است. در ده سال اخیر جورجیا تک در رشته‌های فنی-مهندسی، شهرت زیادی پیدا کرده به طوری که یکی از

---

[۲۱۲] Malmo

[۲۱۳] Internet of Things and People (IOTAP)

[۲۱۴] Georgia Tech

بزرگ‌ترین دانشکده‌های مهندسی در میان تمام دانشگاه‌های آمریکا را امروزه دارا است و در رده‌بندی بهترین دانشکده‌های فنی-مهندسی سال ۲۰۰۷ در ایالات متحده در رتبه چهارم قرار گرفته است.

آزمایشگاه تحقیقاتی CDAIT[۲۱۵] در این دانشگاه با هدف پرورش تحقیقات و تحصیلات، در زمینه‌های بین رشته‌ای IoT، و ایجاد پلی بین این تحقیقات دانشگاهی و صنعت IoT، از بزرگترین مراکز تحقیقات دانشگاهی در زمینه IoT است. در واقع هدف اصلی این مرکز تحقیقاتی، توسعه و گسترش پتانسیل‌ها و توانایی‌های IoT در بخش‌های مختلف کاربردی آن می‌باشد.

### ۳-۴-۶- دانشگاه MIT[۲۱۶]

[http://newsoffice.mit.edu/2012/auto-id-cloud-of-things-big-data]
[http://global.mit.edu/projects/project/the-internet-of-things/]
[http://web.mit.edu/]

مؤسسه فناوری ماساچوست[۲۱۷] (انستیتو[۲۱۸] تکنولوژی ماساچوست) مشهور به MIT ، دانشگاه خصوصی واقع در شهر کمبریج، در ایالت ماساچوست آمریکا است که دارای پنج دانشکده اصلی، یک کالج و ۳۲ گروه آموزشی می‌باشد. این دانشگاه یکی از مهم‌ترین مراکز علمی تحقیقاتی در آمریکا و جهان به شمار می‌رود. دانشگاه MIT همه ساله به عنوان بهترین دانشگاه مهندسی جهان انتخاب می‌شود. MIT در سال ۲۰۱۲ طی الگوی تحقیقاتی انجام شده توسط مؤسسه QS برای رتبه‌بندی کلی دانشگاه‌ها، در رتبه اول بهترین دانشگاه‌های جهان قرار گرفت. دانشکده‌های این دانشگاه عبارت‌اند از: دانشکده علوم، دانشکده فنی مهندس، دانشکده معماری و طراحی، دانشکده مدیریت و دانشکده علوم انسانی، هنر و علوم اجتماعی.

---

[۲۱۵] Center for Development andApplication of Internet of Things

[۲۱۶] MIT

[۲۱۷] Massachusetts

[۲۱۸] Institute

بزرگترین مرکز تحقیقاتی این دانشگاه در زمینه IoT، همان آزمایشگاه معروف RFID می‌باشد که تحت عنوان Auoto-ID شناخته می‌شود. این آزمایشگاه توسط کوین اشتون[۲۱۹]، مبدع واژه اینترنت اشیاء، و سانجای سارما[۲۲۰] احداث شده است. هدف از ایجاد این آزمایشگاه توسیع کدهای تولید الکترونیکی یا سیستم هویت‌یابی RFID-مبنا که جایگزینی برای بارکدها می‌باشد، بود. بسیاری از استانداردهای مربوط به RFIDها و حسگرها توسط این مرکز تحقیقاتی ایجاد شده است. البته پایگاه‌های این آزمایشگاه، امروزه علاوه بر دانشگاه MIT در شش دانشگاه دیگر نیز قرار دارد.

### ۳-۴-۷- دانشگاه کمبریج[۲۲۱]

[http://en.wikipedia.org/wiki/University_of_Cambridge]

دانشگاه کمبریج در شهر کمبریج بریتانیا در کناره رودخانه، واقع شده‌است. این دانشگاه در سال ۱۲۰۹ میلادی تأسیس شده و دومین دانشگاه قدیمی در منطقه انگلیسی زبان و سومین دانشگاه قدیمی در جهان به شمار می‌آید. از آنجا که دانشگاه آکسفورد نیز قدمتی قدیمی دارد، از این رو به این دو دانشگاه، «دانشگاه‌های باستان» می‌گویند و نام آنها را آکسبریج نهادند. کمبریج ۳۱ دانشکده دارد که از این میان، ۳ دانشکده فقط مخصوص خانم‌ها و باقی دانشکده‌ها مختلط است. این دانشگاه در رتبه بندی‌های جهانی همه ساله در بین ۵ دانشگاه برتر دنیا قرار دارد.

مرکز تحقیقاتی Auto-ID دانشگاه کمبریج یکی از هفت مرکزی است که در این زنجیره قرار دارد. تلاش اصلی این مراکز در زمینه هویت‌یابی و دنبال کردن اشیاء است. اهداف اصلی این آزمایشگاه تحقیقاتی به صورت زیر است:

- کاهش عدم اطمینان در تولیدات RFID
- روش‌های دنبال کردن و ردیابی اشیاء
- مدیریت تولید اطلاعات شبکه
- به هم پیوستگی RFIDها با سیستم‌های اتوماتیک و حسگری

---

[۲۱۹] Kevin Ashton

[۲۲۰] Sanjay Sarma

[۲۲۱] Cambridge

این مرکز تحقیقاتی در پروژه‌های زیر که در ارتباط با IoT است، شرکت دارد:

- SAHNE[۲۲۲]
- BRIDGE[۲۲۳]
- عملیات فرودگاهی

### ۳-۴-۸- دانشگاه EPFL

[http://lsir.epfl.ch/research/current/openiot/]

این دانشگاه یک دانشگاه صنعتی است که در شهر لوزان[۲۲۴] کشور سوئیس قرار دارد. EPFL در رتبه‌بندی مجله QS در سال ۲۰۱۴، در بین دانشگاه‌های صنعتی اروپا در رتبه دوم و در بین دانشگاه‌های جهان در رتبه هفدهم قرار گرفت. این دانشگاه دارای ۹۳۰۰ دانشجو از ۱۲۵ کشور جهان است که در مقاطع مختلف در حال تحصیل می‌باشند. دانشکده‌های این دانشگاه عبارتند از: دانشکده علوم، دانشکده مهندسی، دانشکده معماری، مهندسی عمران و محیط زیست، دانشکده علوم مخابرات و کامپیوتر، دانشکده علوم زندگی، کالج مدیریت و تکنولوژی و دانشکده علوم انسانی.

دو آزمایشگاه تحقیقاتی در این دانشگاه در زمینه IoT فعالیت می‌کنند. آزمایشگاه LSIR تحت سرپرستی پروفسور کارل آبرر[۲۲۵] از سال ۲۰۱۱ بر روی پروژه‌ای تحت عنوان OpenIoT، کار می‌کند. OpenIoT یک تلاش مشترک از همکاران منبع-باز[۲۲۶] (شرکت‌های GSN و AspireRFID) برای ایجاد یک شبکه گسترده IoT، با استفاده از مدل محاسبات ابری است.

---

[۲۲۲] Self-serving Asset in Highly Networked Enviroment

[۲۲۳] Building Radio frequency Identification solutions for Global Environment

[۲۲۴] Lausanne

[۲۲۵] Carl Aberer

[۲۲۶] Open-Source

آزمایشگاه بعدی، LCAV می‌باشد که تحت سرپرستی مارتین وترلی[۲۲۷]مدیریت می‌شود. کار اصلی این آزمایشگاه پردازش سیگنال می‌باشد. آزمایشگاه LCAV در زمینه IoT، با تکیه بر مطالعات نظری در حوزه پردازش سیگنال، در تلاش است تا شبکه‌های حسگری را طراحی و مهندسی کند.

تحقیقات اساسی این آزمایشگاه در این زمینه، به صورت زیر می‌باشد:

۱- طراحی یک مدل نرم‌افزاری قابل انعطاف برای شبکه‌های حسگری

۲- افزایش بازدهی-توان و قابلیت اطمینان در شبکه‌های حسگری

۳- نظارت لحظه‌ای بر اطلاعات شبکه‌های حسگری

## ۳-۵- آزمایشگاه‌ها

بعد از آن‌که مطالعات نظری هر تکنولوژی انجام شد، نیاز است که این دانش نظری با واقعیت عملی سازگار شود. در واقع این آزمایش است که حتی می‌تواند مطالعات نظری را در مسیر درست قرار دهد. از این رو آزمایشگاه‌های زیادی در سراسر جهان در حال انجام مطالعات در حوزه IoT هستند. در این بخش به معرفی چهار آزمایشگاه بزرگ، که در حال انجام پروژه‌هایی کلان در زمینه IoT هستند، می‌پردازیم.

### ۳-۵-۱- آزمایشگاه Auto-ID

[http://autoidlabs.org/wordpress_website/]

آزمایشگاه Auto-ID یک گروه تحقیقاتی در زمینه هویت‌یابی فرکانس-رادیویی شبکه شده[۲۲۸] و همچنین فناوری حسگرهای در حال ظهور است. اعضای آزمایشگاه هفت دانشگاه می‌باشد: دانشگاه کمبریج (انگلستان)، دانشگاه MIT (آمریکا)، دانشگاه فودان[۲۲۹] (چین)، مؤسسه تحقیقاتی KAIST[۲۳۰] (کره جنوبی)، دانشگاه کیو[۲۳۱] (ژاپن)، دانشگاه

---

[۲۲۷] Martin Vetterli

[۲۲۸] Networked Radio-Frequency Identification

[۲۲۹] Fudan

[۲۳۰] Korean Advanced Institute of Science and Technology

[۲۳۱] Keio

سنت گالن[۲۳۲] (سوئیس)، دانشگاه آدلاید[۲۳۳] (استرالیا). این مؤسسات برای طراحی و استاندارد سازی معماری IoT و از سال ۱۹۹۹ بوجود آمده‌اند. هدف اصلی این آزمایشگاه استفاده از RFIDها و کد تولید الکترونیکی[۲۳۴] برای هویت‌یابی در زنجیره تولید شرکت‌ها می‌باشد. موضوع تحقیقاتی این آزمایشگاه علاوه بر RFIDها، شامل شبکه حسگرها نیز می‌باشد. تحقیقات این آزمایشگاه به سه بخش سخت‌افزار، نرم‌افزار و تجارت تقسیم می‌شود.

- کاربردهای تجاری:
- گروه تحقیقاتی: دانشگاه سنت‌گالن، دانشگاه کیو، دانشگاه کمبریج، دانشگاه MIT، مؤسسه تحقیقاتی KAIST.
- موارد تجاری
- کاربردهای تجاری
- جنبه‌های امنیت و حریم شخصی
- نرم‌افزار و شبکه
- گروه تحقیقاتی: دانشگاه کیو، دانشگاه MIT و موسسه KAIST
- معماری سیستم‌های آتی
- شبکه EPC
- به هم پیوستگی با شبکه‌های موجود
- سخت‌افزار
  - گروه تحقیقاتی: MIT، دانشگاه فودان، موسسه KAIST
  - طراحی RF و کیت‌های الکترونیکی
  - برچسب‌های حاوی باتری، حافظه و حسگر

---

[۲۳۲] St. Gallen

[۲۳۳] Adelaide

[۲۳۴] Electronic Product Code (EPC)

- افزایش نرخ خواندن اطلاعات

### ۳-۵-۲- آزمایشگاه دانشگاه ویسکانسین[۲۳۵]

[http://www.iotlab.wisc.edu/about-us.aspx]

این آزمایشگاه در یک محیط دانشگاهی (دانشگاه ویسکانسین) قرار گرفته است، که بر روی آموزش، تحقیق و آزمایش در زمینه‌های مختلف اینترنت اشیاء متمرکز است. در واقع در این آزمایشگاه بسیاری از فناوری و ابزارهای نوظهور، به منظور استفاده از کارآیی آن‌ها در پیشبرد IoT، مورد مطالعه قرار می‌گیرد. تیم تحقیقاتی این آزمایشگاه از محققان و اعضای هیئت علمی دانشکده‌های مختلف دانشگاه ویسکانسین می‌باشد: دانشکده برق و کامپیوتر، علوم کامپیوتر، آمار، مهندسی صنایع، مهندسی پزشکی، مهندسی تولید، سیستم‌های اطلاعات، مدیریت، علوم سلامت و بهداشت.

این تیم تحقیقاتی بر روی زمینه‌های مختلف IoT کار می‌کنند، به نحوی که این زمینه‌ها اکثر پژوهش‌های در زمینه IoT را پوشش می‌دهد.

- حسگری
- شبکه، مخابرات و امنیت
- مدیریت داده بزرگ و محاسبات ابری
- تحلیل لحظه‌ای داده
- سیستم تصمیم‌گیری
- مهندسی نرم‌افزار
- علوم انسانی
- طراحی براساس تجربه کاربر
- مهندسی سیستم و فرایند

[۲۳۵] Wisconsin

- مدل سازی تأثیر تجاری

این آزمابشگاه پروژه‌های صنعتی بسیاری را در زمینه IoT هدایت و مدیریت کرده است.

### ۳-۵-۳- آزمایشگاه اشیاء مایکروسافت

[https://labofthings.codeplex.com/documentation]

آزمایشگاه اشیاء، یک پلتفرم قابل انعطاف برای تحقیقات تجربی است که از اشیاء متصل در خانه و بیرون از آن استفاده می‌کند. زمینه‌های تحقیقاتی این آزمایشگاه عبارت اند از :

- ارتباط اشیاء و پیاده سازی سناریوهای کاربری، با استفاده از سیستم عامل خانه[۲۳۶]
- گسترش و نظارت زمینه‌های مطالعاتی و تحلیل داده‌های حاصل از آزمایش
- اشتراک داده‌ها، کدها و محققین برای از میان برداشتن موانع در مسیر IoT

آزمایشگاه اشیاء، طیف گسترده‌ای از تحقیقات را حمایت می‌کند. این تحقیقات می‌توانند در زمینه‌های سلامت، مدیریت انرژی، خانه هوشمند و غیره باشند. با استفاده از زیرساخت ابر آزمایشگاه اشیاء، می‌توان به روز رسانی، ذخیره‌سازی و نظارت بر داده‌ها را عملی نمود.

کار اصلی این آزمایشگاه شامل سیستم عامل خانه و برخی از خدمات ابر است که در پلتفرم آزور توسعه یافت. سیستم عامل خانه روی ویندوز کامپیوترهای شخصی هر خانه یا محیط آزمایشگاهی پیاده‌سازی شد. با استفاده از این فناوری، حسگرها می‌توانند از طریق وای‌فای[۲۳۷] و یا سایر ابزارهای شبکه به کامپیوترهای شخصی متصل شوند. برخی پروژه‌های تحقیقاتی زیر نظر این آزمایشگاه عبارت اند از:

- چند حسگرهای[۲۳۸] پوشیدنی در دستگاه‌های کمکی برای افراد فلج

---

[۲۳۶] HomeOS

[۲۳۷] Wi-Fi

[۲۳۸] Multi-User

- مداخله کینکت-مبنا[۲۳۹] برای بیماران مبتلا به پارکینسون[۲۴۰]
- اشتراک اینترنت اشیاء در خانه‌های هوشمند
- ابزارهای هوشمند برای مدیریت انرژی مصرفی خانه

### ۳-۵-۴- آزمایشگاه IoT اتحادیه اروپا

یک پروژه تحقیقاتی اروپایی است که به تحقیقات روی پتانسیل‌های منابع جمعیتی[۲۴۱] برای توسعه زیر ساخت IoT کمک می‌کند، تا بتوان آزمایش‌های چند رشته‌ای ، با چندین کاربر نهایی را عملی کرد. زمینه‌های تحقیقاتی این آزمایشگاه عبارت اند از:

- ابزارها و مکانیسم منابع جمعیتی: ایجاد امکان استفاده از منبع سوم (تلفن هوشمند) و تعامل با کاربران توزیع شده از طریق یک سیستم، با توانایی حفظ حریم شخصی، مدیریت هویت و امنیت اطلاعات.
- مجازی‌سازی: مجازی‌سازی منابع جمعیتی و ابزارهای متصل برای ایجاد امکان بهره‌وری از به هم پیوستگی تعاملات
- تعامل و امکان محاسبات ابری همه جا حاضر
- کاربر نهایی و ارزش اجتماعی

[۲۳۹] Kinect-base

[۲۴۰] Parkinson

[۲۴۱] Crowdsourcing

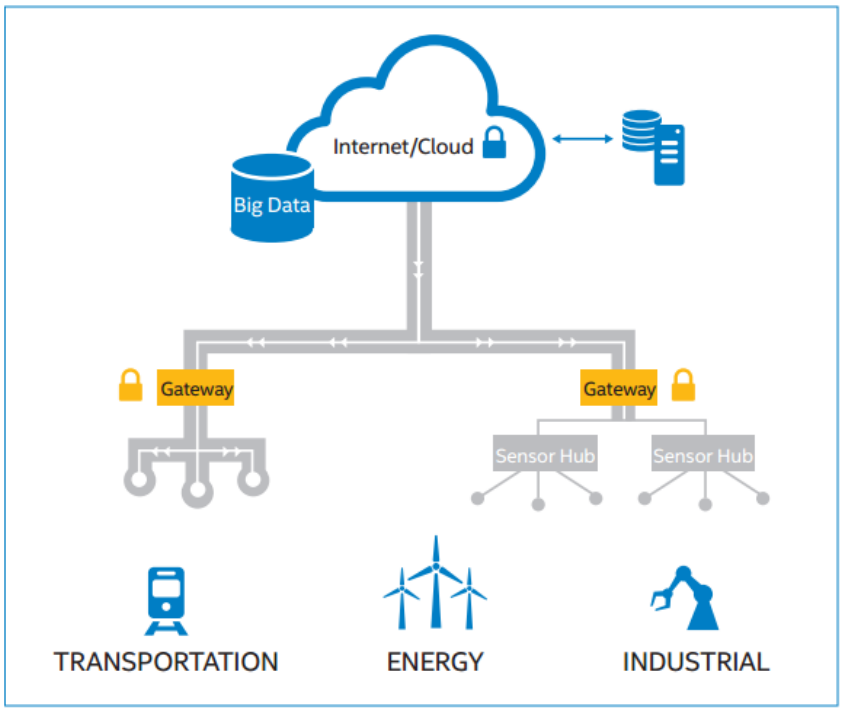
# ۴- معرفی پروژه‌های تحقیقاتی امنیت و حریم خصوصی در اینترنت اشیا

در این بخش به معرفی مختصر مهمترین پروژه‌های تحقیقاتی امنیتی و حریم خصوصی شرکت‌ها، دانشگاه‌ها و مراکز تحقیقاتی مختلف می‌پردازیم. ضمنا پروژه‌های برنامه هفتم توسعه اتحادیه اروپا و برخی پروژه‌های جهانی مهم دیگر را نیز مد نظر قرار می‌دهیم.

## ۴-۱- Intel

http://www.mcafee.com/jp/resources/solution-briefs/sb-intel-gateway-iot.pdf
http://www.intel.com/content/www/us/en/internet-of-things/iot-platform.html

شرکت Intel پروژه‌های متعددی را در زمینه اینترنت اشیاء انجام داده است که هر کدام وصله‌های امنیتی مناسب را با خود دارند. یکی از مهمترین این پروژه‌ها ، درگاه Intel برای اینترنت اشیاء است. درگاه Intel، خانواده‌ای از پلتفرم‌ها است که به شرکت‌ها اجازه می‌دهد تا به صورت بی‌درز[۲۴۲]، به دستگاه‌های صنعتی خود متصل شوند و هم‌زمان، جریان اطلاعاتی بین این دستگاه‌ها و همچنین ابر را امن می‌کند. شکل ۴-۱-۱-۱ محل قرار گیری این درگاه را در شبکه‌ای از اشیاء نشان می‌دهد.




[۲۴۲] Seamless

**شکل ۴-۱-۱-۱ محل قرارگیری درگاه Intel**

این درگاه، برای حفظ امنیت خود از پروتکل‌هایی مثل SSL، امضای دیجیتال، مدیریت گواهی، نظارت بر یکپارچگی، کنترل منابع و ذخیره امن اطلاعات استفاده می‌کند.

پروژه مهم دیگر شرکت Intel در زمینه امنیت اینترنت اشیاء، پلتفرم Intel است. این پلتفرم به طور ویژه، برای رفع تهدیدات امنیتی اینترنت اشیاء طراحی شده تا چالش‌های امنیتی این فناوری را رفع نماید. از جمله مهمترین مزایای پلتفرم Intel، ارائه امنیت به همراه سازگاری[۲۴۳]، مقیاس‌پذیری[۲۴۴] و مدیریت پذیری[۲۴۵] است.

## ۴-۲- مایکروسافت

[http://azure.microsoft.com]

یکی از مهمترین پروژه‌های انجام شده توسط مایکروسافت، پروژه مایکروسافت Azure است. این کاربرد، علاوه بر ارائه ویژگی‌های ارتباطی مناسب برای IoT، امنیت و حریم خصوصی را نیز برای کاربر تأمین می‌کند. در واقع Azure یک پلتفرم چند کاربره است که از یک زیرساخت به اشتراک گذارده شده برای پشتیبانی از میلیون‌ها مصرف کننده همزمان جهت اتصال به بیش از ۸۰ مرکز داده جهانی، استفاده می‌کند. به دلیل به اشتراک گذاری زیرساخت میلیون‌ها ماشین مجازی[۲۴۶] فعال در Azure، حفظ امنیت و محرمانگی ترافیک شبکه بسیار مهم می‌شود. شبکه‌های مجازی Azure ترکیبی از فایروال، کنترل دسترسی، احراز اصالت و رمزنگاری را مورد استفاده قرار می‌دهد تا امنیت داده‌های در حال انتقال کاربران خود را حفظ کند. عملیات مرکز داده Azure، سیاست‌ها و فرایندهای امنیت اطلاعات منسجم را با استفاده از چارچوب‌های کنترل صنعتی استاندارد شده (مثل ISO27001، SOC1 و SOC2) پیاده‌سازی می‌کند. مأموران بی‌طرف نیز به طور منظم، تبعیت مایکروسافت را از این استانداردها (برای جنبه‌های فیزیکی و مجازی

---

[۲۴۳] Interoperability

[۲۴۴] Scalability

[۲۴۵] Manageability

[۲۴۶] Virtual Machine

زیرساخت Azure) گواهی می‌کنند. در مدل قبلی مرکز داده، یک شرکت IT سیستم‌های شبکه شده را با استفاده از دسترسی فیزیکی به تجهیزات شبکه کنترل می‌کند. کارمندان شرکت نیز برای گسترش، پیکربندی و وظایف مدیریتی مثل توپولوژی شبکه هشدار فیزیکی، تغییر تنظیمات مسیریاب، گسترش دستگاه‌های فایروال و غیره مسئولند. در مدل سرویس ابر، مسئولیت حفاظت از شبکه و مدیریت بین ابر و مصرف‌کننده به اشتراک گذارده شده است. مصرف‌کننده‌ها دسترسی فیزیکی ندارند (نمی‌توانند به مرکز داده ابر وارد شوند)، اما می‌توانند معادل منطقی این عملیات را در محیط ابر خود با استفاده از ابزارهایی مثل فایروال‌های سیستم عامل مهمان، پیکربندی درگاه شبکه مجازی، و شبکه‌های خصوصی مجازی، پیاده‌سازی نمایند. این جداسازی فیزیکی و منطقی، مصرف‌کنندگان را قادر می‌سازد تا به قابلیت‌های امنیتی پایه ارائه شده توسط Azure در هنگام ساخت زیرساخت خود اعتماد نمایند.

## ۳-۴ Cisco

مراجع: گزارش سالانه Cisco ۲۰۱۵، و http://www.cisco.com/c/en/us/products/security/index.html

شرکت Cisco امنیت سایبری هوشمند را برای دنیای واقعی فراهم می‌آورد و یکی از جامع‌ترین مجموعه راه‌حل‌های پیشرفته حفاظت از تهدیدات صنعتی را ارائه می‌دهد. محوریت تهدید Cisco و رویکرد عملیاتی به امنیت، پیچیدگی و تقسیم‌بندی[۲۴۷] را کاهش می‌دهد، ضمن اینکه مشاهده‌پذیری بالاتر، کنترل یکپارچه، و حفاظت پیشرفته‌تر را در مقابل تهدید در حین، قبل یا بعد از یک حمله را فراهم می‌کند. محققان امنیتی از سوی اکوسیستم CSI[۲۴۸] در کنار یکدیگر و در زیر یک چتر جمع شده‌اند و با استفاده از سنجش بدست آمده از دستگاه‌ها و حسگرهای عمومی و خصوصی، و اجتماع منبع باز در Cisco، به مقابله با تهدیدات صنعتی می‌پردازند.

روزانه، تخریب میلیاردها درخواست وب و میلیون‌ها ایمیل، فعالیت بدافزارها و مزاحمت‌های مختلف در شبکه رخ می‌دهد. زیرساخت پیشرفته و پیچیده Cisco و سیستم‌های مصرف کننده آن، سیستم‌های یادگیری و محققان را قادر می‌سازد تا تهدیدات شبکه، مرکزهای داده، نقاط پایانی، دستگاه‌های موبایل، سیستم‌های مجازی، وب، ایمیل و

[۲۴۷] Fragmentation

[۲۴۸] Collective Security Intelligence

ابر را دنبال کنند تا علت‌های ریشه‌ای آن‌ها و گستره وقوع آن‌ها را شناسایی نمایند. در این حالت، نتیجه بدست آمده به یک حفاظت آنی برای محصولات و سرویس‌ها تبدیل می‌شود و به تمام مشتریان Cisco در سطح جهان پیشنهاد داده می‌شود. اکو سیستم CSI، ترکیب گروه‌های مختلف با اهداف جدا از هم است، که این گروه‌ها شامل Talos، سازمان امنیت و اعتماد STO[۲۴۹]، دفاع در برابر تهدیدات مدیریت شده MTD[۲۵۰]، و عملیات و تحقیقات امنیتی SR&O[۲۵۱] هستند.

شرکت Cisco محصولات متنوعی را برای پاسخ به نیازمندی‌های امنیتی در قالب پروژه ارائه داده است که از جمله آن‌ها موارد زیر است:

- حفاظت پیشرفته در برابر بدافزارها (AMP[۲۵۲])
- نسل بعدی امنیت شبکه
- امنیت وب و ایمیل
- تحرک‌پذیری[۲۵۳] و دسترسی امن
- مرکز داده امن

### IBM -۴-۴

[Haghighi Report]
[http://www.ibm.com/software/products/en/messagesight]
[http://www.ibm.com/security/xforce/]

IBM کار خود را ذیل پروژه ای به نام Smarter Planet در این زمینه آغاز نمود. در حال حاضر IoT Foundation یک محصول از IBM است که قابلیت‌های ثبت اشیاء (ادوات)، اتصال اشیاء به هم، کنترل اشیاء، نمایش وضعیت اشیاء

---

[۲۴۹] Security & Trust Organization

[۲۵۰] Managed Threat Defense

[۲۵۱] Security Research and Operations

[۲۵۲] Advanced Malware Protection

[۲۵۳] Mobilitiy

و ذخیره داده‌های تولید شده توسط آنها را دارد. به نظر می‌رسد که IBM معماری سرویس‌گرا (SOA) را به دو قسمت شکسته است و لایه‌های زیرین که مربوط به مدیریت اشیاء می‌شوند را ذیل IoT Foundation پیاده سازی نموده که عملا بستری برای اتصال به اشیاء مختلف با میان‌افزارهای مختلف است و اشیاء را کشف و ثبت می‌کند و از دید لایه بالا، پیچیدگی‌های زیرین را مخفی می‌کند.

اما نیمه بالایی پشته پروتکلی SOA مربوط به برنامه‌های کاربردی و ترکیب سرویس اشیاء برای رسیدن به مقصودی خاص است. این بخش در یک محصول دیگر پیاده‌سازی شده است. نتیجه تلاش IBM (در چند حوزه) سکویی بنام Bluemix است که تجاری‌سازی هم شده است. این سکو با ایجاد امکان ارتباط میان دستگاه‌ها (اشیاء)، نوعی بستر برای توسعه برنامه‌های کاربردی بر پایه داده‌ها و آماره‌های به دست آمده از آن‌ها (مانند داده‌های ادوات و سنسورهای شبکه شده) به وجود آورده است. در حال حاضر IBM این محصول خود را به شکل سرویس به فروش می‌رساند و مشتری را بر اساس تعداد تجهیزاتی که قصد اتصال آن‌ها به شبکه را دارد و مقدار ترافیک رد و بدل شده توسط آن‌ها و نیز حجم فضایی که برای ذخیره داده‌های تولیدی اشیاء در ابر مورد نیاز است، شارژ می‌کند.

از دیگر اعضای فعال IBM در زمینه امنیت اینترنت اشیاء، نیروی تحقیق و توسعه X شرکت IBM[۲۵۴] است که یکی از معروف‌ترین تیم‌های توسعه و تحقیق امنیت تجاری در جهان است. این حرفه‌ای‌های امنیتی، موضوعات امنیتی را از انواع منابع شامل پایگاه داده بیش از ۷۶۰۰۰ تهدید امنیتی کامپیوتری، وب جهانی و جمع‌آوری کننده‌های اسپم‌های[۲۵۵] بین‌المللی ارزیابی و نظارت می‌کنند.

تیم نیروی X، گزارش‌های فصلی خود را برای کمک به مشتریان، محققان و کلیه افراد منتشر می‌کند تا آخرین ریسک‌های امنیتی بهتر شناسایی شوند و بهتر در مقابل تهدیدات پدیدار شده، قرار بگیریم. این گزارش‌ها عمیقا به

[۲۵۴] IBM X-Force Research and Development

[۲۵۵] Spam

مهمترین چالش‌های امنیتی که حرفه‌ای ها با آن مواجه می‌شوند، می‌پردازد که شامل تهدیدات نرم‌افزاری و بهره‌برداری عمومی، بدافزار[۲۵۶]، اسپم، فیشینگ[۲۵۷]، تهدیدات بر اساس وب و فعالیت حملات عمومی است.

پروژه دیگری که IBM برای امنیت اینترنت اشیاء انجام داده است، ارائه کاربرد MessageSight برای IoT و محیط موبایل است. این کاربرد یک کانال DMZ-آماده امن برای پیام‌رسانی سبک، سریع و دوطرفه فراهم می‌کند و عملکرد، ارزش و سادگی مورد نیاز برای در بر گرفتن تعداد زیادی از دستگاه‌های موبایل و حسگرها را نیز ارائه می‌دهد.

## ۴-۵- Samsung

[http://www.businesskorea.co.kr/article/6149/samsung%E2%80%99s-future-projects-samsung-selects-10-new-research-items-future-growth]

شرکت سامسونگ در ۲۸ آگوست ۲۰۱۴ اعلام کرد که ۱۰ موضوع تحقیقاتی جدید را در پروژه ارتقای فناوری آینده[۲۵۸] برای امسال در نظر گرفته است؛ پروژه‌ای که در آن سامسونگ حدود 1.4 میلیارد دلار در ۱۰ سال آینده سرمایه‌گذاری خواهد کرد.

موضوعات تحقیقاتی انتخاب شده برای امسال، می‌توانند در سه زمینه ذخیره انرژی، استخراج انرژی از محیط[۲۵۹] و امنیت اینترنت اشیاء دسته‌بندی شوند. با اعطای نام Themes به این سه زمینه توسط سامسونگ، این زمینه‌ها به عنوان زمینه‌هایی از سه دانش پایه فناوری عناصر[۲۶۰]، اطلاعات و ارتباطات قابل تعریف هستند.

در خصوص ذخیره انرژی، این پروژه شامل طراحی عناصر الکترود مثبت جدید برای غلبه بر محدودیت ظرفیت باتری‌های لیتیومی فعلی است. در مورد استخراج انرژی، ایجاد یک مولد روشنایی مصنوعی یکی از زمینه‌های کاری می‌باشد. همچنین در زمینه امنیت IoT نیز امنیت وسیله نقلیه برای مواجهه با هک کردن ماشین‌های هوشمند، نمونه‌ای از چهار پروژه تعریف شده است.

---

[۲۵۶] Malware

[۲۵۷] Phishing

[۲۵۸] Future Technology Promotion Project

[۲۵۹] Energy Harvesting

[۲۶۰] Materials

سامسونگ سال پیش اعلام کرد که اساس ارتقای فناوری آینده را ایجاد خواهد کرد. این شرکت برای پشتیبانی از علوم پایه، مبلغ ۴۹۲ میلیون دلار را در مدت ۱۰ سال در نظر گرفته است و همچنین برنامه دارد تا برای فناوری‌های عناصر، اطلاعات و ارتباطات تا ۹۸۵ میلیون دلار در این مدت سرمایه‌گذاری نماید.

[http://cloudtimes.org/2015/01/21/intel-samsung-cisco-launches-iotivity-open-source-standard-for-the-internet-of-things/]

همچنین به عنوان بخشی از یک کنسرسیوم، سامسونگ با Intel و Cisco همکاری داشته و اولین نسخه از کد استاندارد IoT به نام IoTivity را ارائه داده است. این کد استاندارد مرجع، امکان اتصال دستگاه‌های مختلف از تولیدکنندگان متفاوت را برای ارتباط با یکدیگر فراهم می‌سازد و به این ترتیب، با استاندارد AllJoyn (که توسط Qualcomm، Microsoft و LG ارائه شده،) رقابت می‌کند.

[http://www.rethinkresearch.biz/articles/ibm-samsung-unveil-adept-blockchain-proof-concept-iot-security/]

علاوه بر این، سامسونگ همکاری تنگاتنگی با IBM برای رسیدن به اثبات مفهومی برای ADEPT[۲۶۱] انجام داده است. این سیستم از فناوری زنجیره قالب[۲۶۲] مورد استفاده در Cryptocurrency Bitcoin، برای مدیریت هویت و تراکنش‌های میلیاردها دستگاه پیش‌بینی شده برای IoT بهره می‌برد.

### ۴-۶- SAP

http://iot.stanford.edu/seminar/sitp-w15-sap.pdf

شرکت آلمانی SAP، یکی از شرکت‌های پیشرو در زمینه اینترنت اشیاء است که خروجی‌های بسیاری در این زمینه داشته است. این شرکت، پروژه‌های متعددی را در زمینه امنیت اینترنت اشیاء تعریف کرده است که شامل موارد زیر هستند:

- تعریف سیاست‌های امنیتی آگاه از محتوا

[۲۶۱] Autonomous Decentralized Peer-to-Peer Telemetry

[۲۶۲] BlockChain

- دست امن[۲۶۳]، پروتکلی که تصدیق متقابل یک ویژگی بدون فاش شدن هویت را امکان‌پذیر می‌کند
- ارزیابی اعتماد داده حسگر
- حفاظت از حریم خصوصی برای ردیابی سود در زنجیره تأمین[۲۶۴]
- هشدار امنیتی در زنجیره تأمین
- تبادل امن داده ردیابی RFID
- حریم خصوصی در سیستم‌های فیزیکی سایبری
- چندکاربره بودن حسگرهای مورد استفاده در ساختمان دفاتر رسمی
- تحلیل قابل پیش‌بینی برای یکپارچگی متوالی[۲۶۵]

پروژه‌های امنیتی فوق، در کاربردهای ارائه شده توسط شرکت SAP مورد توجه قرار گرفته است. از جمله مهمترین دستاورد این شرکت در زمینه اینترنت اشیاء، پلتفرم HANA است که امنیت این پلتفرم نیز با بهره‌گیری از خروجی پروژه‌های امنیتی این شرکت تأمین می‌شود. از دیگر پروژه‌های امنیتی مهم شرکت SAP موارد زیر هستند:

- محک حفظ حریم خصوصی در ابر
- مدیریت مشارکتی امن زنجیره تأمین
- سیستم‌های اعتباری ارتجاعی[۲۶۶]
- جستجو روی داده‌های رمز شده

## ۴-۷- Oracle (پروژه معماری Oracle برای IoT)

[Internet of things security architecture, Noel Poore, Architect, Java Platform Group, September 29, 2014]

---

[۲۶۳] Secure handshake

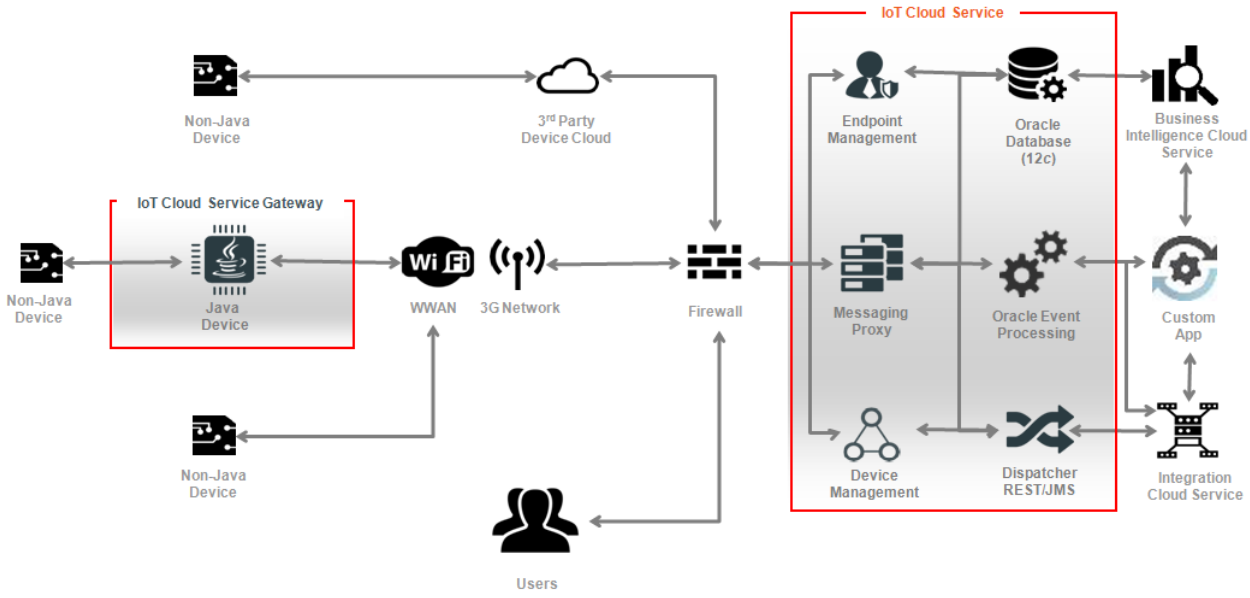
[۲۶۴] Supply chain

[۲۶۵] Pipeline integrity

[۲۶۶] Resilient reputation

مهمترین پروژه شرکت Oracle برای IoT، معماری پیشنهادی این شرکت برای اینترنت اشیاء است. شکل ۴-۷-۱-۱ شمای کلی معماری شرکت Oracle را برای IoT نشان می‌دهد. در این معماری، کاربران، ابر و شبکه ارتباطی توسط یک فایروال مرکزی به یکدیگر متصل می‌شوند. در این معماری، داده‌های دریافتی از IoT از مسیر فایروال وارد ابر می‌شود و پس از پردازش کنترل‌های لازم به آن‌ها باز می‌گردد. به منظور امن کردن این معماری، اصول اولیه‌ای مورد نظر شرکت Oracle بوده است که از جمله مهمترین آن‌ها، موارد زیر است:

- دسترسی به دستگاه‌ها و کاربردها (از هر مکان در شبکه IoT)
- دسترسی به داده‌های تولید شده (چه این داده‌ها در حرکت و چه ثابت باشند)




شکل ۴-۷-۱-۱ معماری Oracle برای IoT

## ۴-۸ ARM: پروژه mbed

[https://mbed.org/]

در اینترنت اشیاء به دنبال راه‌حل‌های پایان به پایان رساندن سرویس‌ها به دستگاه‌ها هستیم. به این منظور شرکت ARM یک پلتفرم IoT به نام mbed پیشنهاد کرده است که به ادعای خود، سریع‌ترین راه برای ایجاد یک اتصال تجاری و سازگار میان دستگاه‌های IoT بر اساس میکروکنترلرهای ARM است.

در صورت وجود سازگاری میان نودها و سرویس‌های ابر در بخش‌های مختلف بازار، پتانسیل کامل IoT را نمایان می‌شود. اگرچه بازار IoT از بخش‌های مستقل از هم تشکیل شده است، اما بسیاری از کاربردها که می‌توانند از دستگاه‌های متصل شده به اینترنت استفاده نمایند، یک پایه مشترک دارند. برای مثال، شهرهای هوشمند، دستگاه‌های هوشمند و خانه هوشمند به توابع پایه سیستم عامل مثل درایورها، امنیت دستگاه و پشتیبانی از تدارکات احتیاج دارند. علاوه بر این، اتصالات شبکه از کاربرد به کاربرد تغییر می‌کند و به طور کلی، نیازهای شبکه‌بندی با IP، امنیت، لایه کاربرد و مدیریت دستگاه همگی مشترک هستند.

پلتفرم mbed شرکت ARM تمام اجزای کلیدی مورد نیاز برای ساخت یک کاربرد IoT کارا و امن را در یک سیستم عامل ARM، سرور mbed و اکوسیستم اجتماع mbed فراهم می‌آورد. در واقع با پلتفرم mbed به مزایای زیر دست پیدا می‌کنیم:

- پاسخ به مسأله تکه‌تکه کردن در طراحی فشرده به وسیله ارائه یک سیستم عامل مشترک برای دستگاه‌های IoT
- امکان طراحی‌ها با تضمین آینده[۲۶۷] به وسیله پشتیبانی از تمام استانداردهای کلیدی باز برای اتصال و مدیریت دستگاه
- امکان ارائه دستگاه‌های امن و قابل بروز رسانی در لبه قابلیت‌های پردازشی و تابعی
- پاسخ به مسأله دشوار مصرف توان به وسیله ایجاد مدیریت توان اتوماتیک
- ایجاد ابزار توسعه بر اساس ابر که ایجاد محصول را سرعت می‌بخشد
- کنار هم جمع کردن شرکت‌های فناوری فشرده و ابر به همراه اجزاء سازنده، تجمیع کننده‌های سیستم و OEM[۲۶۸]ها که می‌خواهند سرویس‌ها، ابزارها و فناوری‌های مورد نیاز را برای تسریع نوآوری در خلق و گسترش سیستم‌های IoT فراهم آورند.

[۲۶۷] Future Proof Designs

[۲۶۸] Original Equipment Manufacturer

## ۴-۹- پروژه‌های امنیت اینترنت اشیاء در برنامه هفتم توسعه اتحادیه اروپا (FP7)

در این زیربخش، پروژه‌های امنیتی مرتبط با اینترنت اشیاء در اتحادیه اروپامورد بررسی قرار می‌گیرد که این پروژه‌ها، توسط چارچوب برنامه ۷ ام اتحادیه اروپا (FP7) پشتیبانی می‌شوند.

### ۴-۹-۱- پروژه Elliot

[http://www.elliot-project.eu]

هدف پروژه Elliot[۲۶۹]، توسعه یک پلتفرم تجربی IoT است که کاربران/شهروندان مستقیما در ایجاد آن مشارکت کنند و ایده‌ها ، مفاهیم و محصولات فنی جدید مرتبط با کاربردها و سرویس‌های IoT را کشف و تجربه نمایند. این پروژه، اثر IoT و اینترنت آینده را در زمینه "پارادایم نوآوری مرکزی شده کاربر باز[۲۷۰]" و "رویکرد آزمایشگاه زندگی[۲۷۱]" مطالعه می‌کند.

رویکرد تجربی Elliot قبلا نیز استفاده شده است و پلتفرم فناوری آن در موقعیت‌های استفاده مختلف مربوط به ۶ بخش مختلف با نام‌های تندرستی[۲۷۲]، منطق[۲۷۳]، محیط[۲۷۴]، خرده‌فروشی[۲۷۵]، کمک از راه دور به بیماران[۲۷۶] و دفتر کارایی انرژی[۲۷۷] آزمایش شده است تا ظرفیت موجود برای کاربران/شهروندان برای همکاری در ایجاد سرویس‌های بر پایه IoT ارزیابی شود. با شروع از این ۶ موقعیت، پروژه Elliot می‌تواند در یک رویکرد جدید و کاربر محور برای

---

[۲۶۹] Experiential Living Lab for the Internet of Things

[270] Open User Centred Innovation paradigm

[۲۷۱] Living Lab approach

[۲۷۲] Wellbeing

[۲۷۳] Logistic

[۲۷۴] Environment

[۲۷۵] Retail

[۲۷۶] Remote Patients Assitance

[۲۷۷] Energy Efficient Office

توسعه سرویس/محصول جدید در اینترنت اشیاء با پلتفرم IoT تجربی خود همکاری نماید که بسیار مناسب برای گسترش تصاعدی به دیگر بخش‌ها و دامنه‌های صنعتی نیز هست.

در پایان این پروژه، همه ویژگی‌ها و مدل‌های نمونه در یک پلتفرم نهایی یکپارچه‌سازی خواهند شد و به عنوان یک پایه دانش مهم و گسترده برای ارزیابی، تصدیق و اعتبارسنجی خروجی‌های Elliot مورد استفاده قرار می‌گیرند.

### ۴-۹-۲- uTrustIT

[http://www.utrustit.eu/]

پروژه uTrustIT یک پروژه مشترک بین ۶ کشور برای ایجاد یک زنجیره اعتماد میان کاربران خود است تا بتوانند شفافیت لازم را در امنیت و قابلیت اعتماد IoT ایجاد کنند. این پروژه توسط اتحادیه اروپا و تحت چارچوب برنامه هفتم (FP7) پشتیبانی می‌شود.

نتایج حاصل از این پروژه تولیدکنندگان سیستم‌ها را قادر خواهد ساخت تا مفاهیم امنیتی به شیوه‌ای منسجم‌تر برای کاربران بیان کنند و به آنها اجازه دهند تا خودشان در مورد اعتماد به سیستم آن‌ها تصمیم‌گیری نمایند. همچنین، راهنمای طراحی uTrustIT در مورد اعتماد، به صنعت کمک می‌کند تا toolkit اعتماد طراحی شده توسط این پروژه را به شیوه امن، قابل استفاده و در دسترس پیاده‌سازی کنند.

### ۴-۹-۳- پروژه Smartie

[http://www.smartie-project.eu/project.html]

**اهداف اصلی این پروژه به این شرح است:**

- شناسایی نیازمندی‌ها برای امنیت داده و کاربرد، و ایجاد یک چارچوب مناسب برای پشتیبانی از به اشتراک‌گذاری داده در میان کاربردها
- ایجاد و توسعه فناوری‌های جدید که بتواند اعتماد و امنیت را در لایه مفهومی و لایه شبکه ایجاد نماید

- ایجاد و توسعه فناوری‌های جدید برای ایجاد اطلاعات مورد اعتماد، و ذخیره‌سازی امن برای لایه سرویس اطلاعات[۲۷۸]
- ایجاد فناوری‌های جدید برای بازیابی و پردازش اطلاعات که توسط سیاست‌های کنترل دسترسی در لایه کاربرد هدایت می‌شوند.
- بیان نتایج پروژه در موقعیت‌های استفاده عملی

### ۴-۹-۴- پروژه IoT-A، معماری اینترنت اشیاء

[http://www.iot-a.eu/public]

اینترنت اشیاء موضوعات متعامدی را مد نظر قرار می‌دهد که سازگاری و تعامل‌پذیری را پشتیبانی نمی‌کنند. با این حال، تلاش‌های متعددی برای ایجاد این ویژگی انجام شده است، اما راه‌حل‌های ارائه شده، مقیاس‌پذیر نیستند تا برای آینده اینترنت اشیاء مناسب باشند. ضمن اینکه به طور ویژه، مباحث امنیت و حریم خصوصی نیز در طراحی این پاسخ‌ها لحاظ نشده است.

IoT-A (پروژه اتحاد فانوس اروپا[۲۷۹]) در مدت سه سال، به مسأله معماری اینترنت اشیاء پاسخ داد و یک مدل مرجع معماری را به همراه تعریف اولیه جعبه‌های سازنده اصلی[۲۸۰] آن ایجاد کرد که به عنوان پایه‌ای برای پرورش نوآوری در ظهور اینترنت اشیاء دیده می‌شود. با استفاده از یک تجربه، IoT-A با ترکیب استدلال‌های اصول معماری، یک راهنما به همراه شبیه‌سازی ارائه داد و یک نمونه اولیه برای شناسایی نتایج فنی انتخاب‌های طراحی معمارانه منتشر کرد.

به منظور دستیابی به یک معماری پایه برای اینترنت اشیاء، IoT-A مجموعه‌ای از اهداف فنی و علمی را مشخص کرده است که به این شرح هستند:

---

[۲۷۸] Information Service Layer

[۲۷۹] The European Lighthouse Integrated Project

[۲۸۰] Key Building Blocks

- ارائه یک مدل مرجع معماری برای سازگاری[۲۸۱] سیستم‌های IoT، با بیان اصول و راهنماها برای طراحی فنی پروتکل‌ها، رابط‌های کاربری و الگوریتم‌های آن
- ارزیابی تقاضاهای پروتکل IoT موجود و استخراج مکانیزم‌هایی برای رسیدن به سازگاری (تعامل‌پذیری) پایان به پایان برای ارتباطات بی‌درز میان دستگاه‌های IoT
- ایجاد و توسعه ابزارهای مدل‌سازی و زبان توصیف برای تراکنش‌های IoT که امکان بیان وابستگی‌های آن‌ها را برای مجموعه‌ای از مدل‌های گسترش گوناگون فراهم سازد
- استنتاج مکانیزم‌های وفقی برای هماهنگی توزیع‌شده تراکنش‌های منابع IoT که ویژگی‌های خود را به منظور سر و کار داشتن با تغییرات پیچیده محیط واقعی، افشا می‌کنند
- ایجاد مکانیزم‌ها حریم خصوصی و امنیت کارا و کل نگرانه در دستگاه‌های IoT و پروتکل‌ها و سرویس‌های مورد استفاده آن‌ها
- ایجاد و توسعه یک زیرساخت تفکیک[۲۸۲] جدید برای IoT که امکان کشف منابع IoT، نهادهای دنیای واقعی و موارد وابسته به آن‌ها را به صورت مقیاس‌پذیر فراهم کند
- ایجاد و توسعه اجزای پلتفرم دستگاه IoT شامل سخت‌افزار و محیط اجرا
- ارزیابی مدل مرجع معماری در مقابل نیازهای استنتاج شده با پیاده‌سازی آن در دنیای واقعی و مشاهده فواید راه‌حل‌های مطرح شده
- مشارکت در پخش و بهره‌برداری از پایه‌های معماری ایجاد شده

### ۴-۹-۵- COMPOSE[۲۸۳]

[Haghighi Report]

[B. Mandler, *Final COMPOSE architecture document*, IBM & European Commission, 2014.]

---

[۲۸۱] Interoperability

[۲۸۲] Resolution Infrastructure

[۲۸۳] Collaborative Open Market to Place Objects at your Service

هدف COMPOSE تبدیل اینترنت اشیاء به اینترنت سرویس‌ها است. COMPOSE این کار را با ایجاد زیرساخت بازاری باز و قابل توسعه انجام می‌دهد. در این بازار اشیاء هوشمند به سرویس‌ها نسبت داده شده و این سرویس‌ها می‌توانند به شکلی استاندارد با هم ترکیب شده، مدیریت شوند تا بتوان به راحتی برنامه‌های کاربردی نوین به وجود آورد. در واقع دید COMPOSE ایجاد یک اکوسیستم تجاری بوده است که بین اینترنت اشیاء، اینترنت محتوا (داده) و اینترنت سرویس‌ها همگرایی ایجاد کند. این پروژه در نوامبر ۲۰۱۲ آغاز شده و طول آن ۳ سال پیش‌بینی شده است. بودجه‌ای که برای این پروژه در نظر گرفته شده ۷,۴ میلیون یورو است و ذینفع اصلی آن IBM می‌باشد. با این وجود این پروژه ذیل برنامه هفتم توسعه اتحادیه اروپا در حوزه ICT انجام می‌شود (FP7-ICT). معماری و چارچوب طراحی شده در دو شهر Barcelona و Trentino به صورت پایلوت اجرا می‌شوند. اهم خروجی‌های این پروژه عبارتند از:

- طراحی یک معماری برای اینترنت اشیاء
- طراحی شاخص‌های لازم برای مجازی‌سازی اشیاء (خلاصه‌سازی)
- طراحی شاخص‌ها و اجزای لازم برای ترکیب (خدمات) اشیاء
- طراحی و تعریف معماری امنیتی برای اینترنت اشیاء
- شناسایی و تحلیل نیازمندی‌های برخی موارد کاربرد (Use case)
- طراحی رابط‌ها و نحوه اجرای سرویس
- ساخت نمونه پایلوت
  - ایجاد API برای توسعه‌دهندگان برنامه کاربردی (SDK & IDE & API)
  - پیاده‌سازی آزمایشی اجزای شناسایی سرویس‌ها، ثبت سرویس‌ها، ترکیب سرویس‌ها، محیط اجرای سرویس و نیز مدیریت هویت
  - پیاده‌سازی آزمایشی توصیه کننده سرویس (Service Recommender)
- تحلیل مدل کسب و کار بر اساس معماری COMPOSE

## ۴-۱۰- پروژه‌های دیگر

در این بخش پروژه‌های دیگر امنیتی مرتبط با اینترنت اشیاء که با مشارکت مراکز تحقیقاتی و شرکت‌های مختلف در حال انجام هستند (یا به پایان رسیده‌اند) بررسی می‌شود.

### ۴-۱۰-۱- OWASP (Open Web Application Security Project)

این پروژه ۱۰ مسأله امنیتی مهم مرتبط با اینترنت اشیاء را مد نظر قرار می‌دهد که در بخش ۳-۱-۲- به آن پرداخته شد. همچنین لیستی از توصیه‌های امنیتی پایه را نیز برای تولیدکنندگان، توسعه‌دهندگان و مصرف کنندگان ارائه می‌دهد. همچنین برای هر حمله باید بخش‌های زیر در این پروژه مورد بررسی قرار بگیرد:

۱- توصیف حمله

۲- تهدیدات

۳- بردارهای حمله

۴- ضعف‌های امنیتی

۵- آثار فنی

۶- آثار تجاری

۷- مثال برای آسیب‌پذیری

۸- مثالی از حمله

۹- راهنمایی برای جلوگیری از حمله

۱۰- ارجاع به OWASP و منابع وابسته

همچنین برای هر نقش در تولیدکننده، توسعه‌دهنده و مصرف‌کننده نیز بایستی مهمترین نقطه نظرات که باید در محتوا مشاهده شوند، لیست شوند.

### ۴-۱۰-۲- Secure Internet of Things Project (SITP)

مدت زمان این پروژه ۵ سال است (از سال ۲۰۱۴) و ۱۲ استاد دانشگاه از دانشگاه‌های استنفرد، برکلی و میشیگان انجام آن را بر عهده دارند. این پروژه دو هدف عمده دارد که به این ترتیب هستند:

۱- امنیت داده: تحقیق و تعریف مدل‌های جدید محاسباتی رمزنگاری برای تحلیل امن داده‌ها و راه‌اندازی روی دنباله‌های داده آنی بزرگ از سیستم‌های فشرده

۲- امنیت سیستم: تحقیق و پیاده‌سازی یک چارچوب نرم‌افزاری/سخت‌افزاری باز و امن که استفاده از این مدل‌های جدید محاسباتی را در ساخت کاربردهای اینترنت اشیاء، سهولت بخشد.

### ۴-۱۰-۳- پروژه BUTLER

[http://www.iot-butler.eu/about-butler]

شرکای پروژه BUTLER شامل ۱۷ شریک از ۸ کشور جهان است که با یک همکاری صنعتی قوی (۶ مؤسسه آکادمیک و ۱۱ شرکت) کار خود را آغاز کرده‌اند. این پروژه، اولین پروژه اتحادیه اروپا است که به فراگیری[۲۸۴]، آگاهی از محتوا[۲۸۵] و امنیت برای IoT تأکید دارد. این پروژه فناوری‌های جدید را به شکل یک مجموعه کامل[۲۸۶] تجمیع نموده و روی موارد زیر تمرکز کرده است:

- ایجاد/بهبود فناوری‌های تواندمندساز برای اجرایی کردن یک دیدگاه تعریف شده از امنیت، فراگیری و آگاهی از محتوا در IoT که ارتباطات آن کاربردهای امنیتی (از لایه فیزیکی تا کاربرد) در سناریوهای مختلف (خانه، محل کار، حمل و نقل، بهداشت و غیره) هستند، و بازخوردهای شبکه به کاربران، تنظیم نیازهای آن‌ها (آموزش و نظارت به صورت آنی) هستند.
- تجمیع/توسعه یک معماری شبکه مرکزی انعطاف‌پذیر جدید که وظایف دستگاه‌ها و پلتفرم‌های آن بر طبق سه دسته زیر است: اشیاء هوشمند (حسگرها، درگاه‌ها، فعال‌کننده‌ها)، موبایل‌های هوشمند (دستگاه‌های

---

[۲۸۴] Pevasive

[۲۸۵] Context awareness

[۲۸۶] Bundle

شخصی کاربران) و سرورهای هوشمند (ارائه کننده محتوا و سرویس) که توسط IPv6 به یکدیگر متصل شده‌اند.

- ساختن یک سری آزمایش‌های میدانی که به صورت دنبال هم، فناوری‌ها را به سوی اهداف BUTLER سوق می‌دهند.

### ۴-۱۰-۴- پروژه Ebbits

[Haghighi Report]

پروژه Ebbits[۲۸۷] در زمینه معماری، فناوری و فرآیندهایی تحقیق می‌کند که به کسب و کارها اجازه می‌دهد تا بصورت معنایی[۲۸۸] اینترنت اشیاء را به جریان اصلی کار سامانه‌های سازمان و یا شرکت متصل نموده و به صورت تعامل‌پذیر برنامه‌های کاربردی تجاری را (روی آن) به صورت سرتاسری اجرا کنند.

هدف اصلی در Ebbits ایجاد یک سکو برای دارندگان کسب و کار برای استفاده از پتانسیل‌های اینترنت اشیاء است. سکوی پیشنهادی در پروژه Ebbits از معماری سرویس‌گرا (SOA) تبعیت کرده و از پروتکل‌ها و میان‌افزارهای (متن) باز استفاده می‌کند. این مسأله به Ebbits اجازه می‌دهد که تقریبا هر دستگاه و یا سامانه‌ای را به یک وب-سرویس تبدیل کند. این پروژه در فوریه ۲۰۱۵ پایان یافت.

### ۴-۱۰-۵- پروژه EPoSS

[Haghighi Report]

پروژه EPoSS[۲۸۹] در حقیقت به جنبه فنی اینترنت اشیاء نمی‌پردازد، بلکه به خلاء سیاستگذاری و تحقیق و تعریف پروژه‌های لازم برای آن می‌پردازد. بطور دقیق‌تر، EPoSS یک پروژه است که هدف آن تعریف نیازمندی‌های تحقیق

[۲۸۷] Enabling the Buiness-based Internet of Things and Services

[۲۸۸] Semantically

[۲۸۹] The European Technology Platform on Smart Systems Integration

و توسعه‌ای و نیز سیاستگذاری برای اتصال و یکپارچه‌سازی سامانه‌های هوشمند و متجمع‌سازی سامانه‌های خرد است. این پروژه بخشی از تلاش اتحادیه اروپا برای تحقق چشم انداز ۲۰۲۰ این اتحادیه است.

EPoSS رویکرد یکسانی را در سطح اروپا برای اتصال و یکپارچه‌سازی سامانه‌های هوشمند از مرحله تحقیق تا ساخت ارائه می‌کند. همچنین اولویت‌های تحقیق را برای آینده معرفی کرده و انسجام و هماهنگی لازم را برای به مرحله عمل درآوردن نقشه راه‌های توافق شده در اتحادیه به وجود می‌آورد. علاوه بر این، یک برنامه (پلان) تحقیقاتی استراتژیک را (در زمینه سیستم‌های هوشمند) ارائه کرده و مانند پلی بین تلاش‌های تحقیقاتی بخش‌های خصوصی و دولتی در این زمینه عمل می‌کند. حامیان این پروژه تقریبا از ۲۰ کشور اتحادیه اروپا هستند و در میان آنها شرکت‌های صنعتی، دانشگاه‌ها، و حتی کمیسیون اتحادیه اروپا دیده می‌شوند (شکل ۴-۱۰-۵-۱).


**شکل ۴-۱۰-۵-۱ حامیان پروژه EPoSS**

به نظر می‌رسد با توجه به نقش و دایره وظایف EPoSS، مطالعه و بررسی این پروژه برای جایگاه راهبردی مرکز تحقیقات مخابرات ایران مفید باشد و چنانچه در کشور ما حرکت به سوی اینترنت اشیاء آغاز گردد، نیاز به وجود چنین نهادی احساس خواهد شد.

# ۵- نیازمندی‌های امنیتی اینترنت اشیاء

[http://www.iot-a.eu/public]

لزوم برقراری امنیت در اینترنت اشیاء واضح است. جهت چنین امری، نیازمند برخی موارد هستیم. در این بخش این نیازمندی‌ها مطرح می‌شوند. ما نیازمندی‌های حریم‌خصوصی و اعتماد را از نیازمندی‌های امنیتی جدا کردیم و به طور مجزا به آن‌ها پرداخته‌ایم. لازم به ذکر است که نیازمندی‌های امنیتی به طور کلی باید به صورت قانون در بیایند و لازم الاجرا باشند تا بتوان سیاست‌های امنیتی اینترنت اشیاء را در عمل پیاده‌سازی نمود.

## ۵-۱- نیازمندی‌های امنیتی

به طور کلی، نیازمندی‌های امنیتی اینترنت اشیاء شامل موارد زیر است:

۱- تضمین ایمنی زندگی انسان‌ها (Safety of Human Lives)

۲- جلوگیری از زنجیره حوادث نامطلوب

۳- در دسترس بودن سیستم (System Availability)

۴- محرمانگی و یکپارچگی اطلاعات (Confidentiality & Integrity)، رمزنگاری و فناوری‌های حفاظت داده کارا از نظر انرژی

۵- امضای دیجیتال و انکارناپذیری

۶- سازگاری اطلاعات و سطوح امنیتی آن‌ها در سیستم‌های مختلف

۷- شناسایی (به طور یکتا)، احراز هویت اشیاء و اشخاص (چند عاملی مثل پسورد، مکان، بیومتریک، اثبات هیچ دانشی)، و قابلیت نسبت دادن هر شیء تنها به یک شخص

۸- مدل‌های مختلف برای اعتماد و احراز هویت غیر مرکزی

۹- احراز هویت پیام‌های ارسالی

۱۰- نظارت، بازرسی، مدیریت امنیتی، و کنترل دسترسی (حقوق دسترسی و استفاده، قوانین به اشتراک گذاری ارزش افزوده) و صدور مجوز

۱۱- مدیریت، تبادل و توافق کلید برای امکان آغاز ارتباط امن

۱۲- حفاظت فیزیکی و منطقی از اطلاعات

۱۳- امنیت سخت‌افزاری و نرم‌افزاری (امنیت ارتباط بی‌سیم در لایه فیزیکی) به صورت پایان به پایان

۱۴- امنیت و اعتماد برای محاسبات ابری

۱۵- مشخص کردن پروتکل و الگوریتم مورد استفاده برای گیرنده ضمن حفظ امنیت آن

۱۶-ثبت کردن و ارائه گزارش (Log & Report)

۱۷- قابلیت پیاده‌سازی در محیط‌های محدود با قدرت پردازش و حافظه پایین

۱۸- کمینه کردن مصرف توان و هزینه سربار امنیتی، و آگاهی از میزان مصرف انرژی در دستگاه‌ها توسط مراجع ذی‌صلاح

۱۹- حفاظت در برابر هک، نفوذ، مرد در میانه

۲۰- حفاظت در برابر DoS، DDoS و Sybil

۲۱- حفاظت در برابر حملات لایه شبکه مثل حملات مسیریابی مسیریابی، لانه کرمی، سیاهچاله و غیره

۲۲- حفاظت در برابر حمله تکرار، حمله اثرانگشت و پروفایل‌گیری

۲۳- حفاظت در برابر فیشینگ، شنود، اختلال (Jamming)، تغییر و استخراج اطلاعات

۲۴- تضمین مالکیت داده، دستگاه یا شیء برای افراد

۲۵- موضوعات قانونی و مسئولیتی، ارائه چارچوب و سیاست‌های امنیتی و حریم‌خصوصی

۲۶-پذیرش مسئولیت‌پذیری برای انجام برخی عملیات توسط کاربر

۲۷- مدیریت مخزن داده

۲۸- دستگاه‌های کم‌هزینه و امن

۲۹- اولویت‌دهی پیام‌ها و اطمینان از ارسال و دریافت پیام‌ها بر اساس اولویت‌شان

۳۰- امکان کشف یا عدم کشف یک دستگاه در هنگام جستجوی آن

۳۱- بررسی محتوا برای شناسایی تخریب (مثلا برای محتواهای ساده مثل اندازه‌گیری دما یا رطوبت)

۳۲- استفاده از مکانیزم‌های اعتباردهی برای کشف تخطی

۳۳- تضمین قابلیت اطمینان عملکرد سیستم

۳۴- بررسی میزان سطح خودمختاری مورد نیاز برای مدیریت امنیتی توسط سیستم

۳۵- اطمینان از عملکرد صحیح تمامی فعالیت‌های لایه‌های شبکه در سیستم

۳۶- بررسی اثر تاریخچه[۲۹۰] ذخیره شده در کاربردها در امنیت سیستم

۳۷- بررسی استفاده از Bridge در برخی موارد لازم برای حفظ امنیت یا حریم خصوصی

۳۸- بررسی اثر تحرک‌پذیری در امنیت سیستم

۳۹- استفاده از هویت یکتا در سطح جهانی برای شناسایی

۴۰- لایه امنیت باید مستقل از لایه‌های دیگر و قابل جایگزینی و تعویض باشد

۴۱- تازگی[۲۹۱] و انصاف[۲۹۲]

طبیعی است که نیازمندی‌های طبیعی به ذکر این موارد ختم نمی‌شود و رفع هر تهدید موجود در IoT، به نوعی یک نیازمندی امنیتی محسوب می‌شود. لذا سیستم IoT باید در برابر تمام حملات موجود و حملات آینده‌ای که به دلیل ساختار جدید IoT شکل خواهند گرفت، مقاوم باشد.

همچنین نیازمندی‌های امنیتی بر اساس لایه شبکه و نوع کاربرد متفاوت هستند و استخراج دقیق این نیازمندی‌ها بنا بر شرایط، نیازمند بررسی بسیار کلی و جامع است. از جمله شرایطی که نیازمندی‌های امنیتی در آن‌ها می‌تواند متفاوت باشد، مانند استفاده از RFID، شبکه‌های حسگری، سیستم‌های وایرلس، شبکه‌های پوششی، سیستم‌های بی‌درنگ، سیستم‌های قابل اطمینان، بسترهای فیزیکی و منطقی ارسال اطلاعات، درگاه‌های ارتباطی، ساختار شبکه (مرکزی و غیرمرکزی)، تعداد عناصر و ساختار آنها، میزان اهمیت یک سیستم یا دستگاه، مسیریابی، ترافیک‌های عبوری و ازدحام، و پروتکل‌های امنیتی مورد استفاده است.

---

[۲۹۰] History

[۲۹۱] Freshness

[۲۹۲] Fariness

هر چالش امنیتی موجود برای IoT نیز خود یک نیازمندی امنیتی را معرفی می‌کند که در بخش چالش‌ها بیشتر به آن پرداخته می‌شود.

## ۵-۲- نیازمندی‌های حریم خصوصی

اگرچه حریم خصوصی، خود زیر مجموعه نیازمندی‌های امنیتی در نظر گرفته می‌شود، اما در اینجا به طور جداگانه بررسی می‌شود. دلیل این امر، اهمیت بالقوه این مسأله است، چرا که عدم حفظ حریم خصوصی موجب عدم پذیرش سیستم توسط مردم می‌شود که در نتیجه هدف نهایی از میان می‌رود. مقوله حریم خصوصی در اینترنت اشیاء بسیار حیاتی‌تر است. برخلاف اینترنت معمولی، حجم اطلاعات اندازه‌گیری شده (از افراد یا توسط افراد) بسیار بالاتر است و بنابراین خطر افشای اطلاعات شخصی افراد به مراتب بیشتر است. اطلاعات شخصی افراد می‌تواند شامل:

**مکان، اطلاعات اکتسابی (مثل مدرک تحصیلی، همسر)، اطلاعات ذاتی (مثل جنسیت، نام)، مهارت‌های فردی، پروفایل رفتاری، علاقه‌مندی‌ها، اطلاعات شغلی، دارایی‌ها و مالکیت‌های یک شخص از اشیاء، پیشینه**

و بسیاری از موارد دیگر باشد که همه آن‌ها باید با رضایت شخص به مراجع معتبر تحویل داده شود و هیچگونه درز اطلاعات در این موارد توسط اشخاص قابل قبول نیست. حسگرها و دستگاه‌های مشارکت کننده در اینترنت اشیاء، به راحتی می‌توانند به این اطلاعات دسترسی پیدا کنند و در نتیجه حفاظت از این اطلاعات در این دستگاه‌ها بسیار حیاتی خواهد بود.

از طرف دیگر، مقوله حریم خصوصی، با گمنامی و استفاده از نام مستعار تفاوت‌هایی دارد. استفاده از نام مستعار به دلایل امنیتی می‌تواند مورد استفاده قرار بگیرد. همچنین در حفظ حریم خصوصی، فرد باید برای دشمنان گمنام بماند، ضمن اینکه باید بتواند خود را به افراد معتبر معرفی نماید. در برخی کاربردها برخی ویژگی‌های لازم و مرتبط با حریم خصوصی باید به طور همزمان ایجاد شوند، به عنوان مثال گمنامی و تأیید اعتبار یک شخص باید به طور همزمان صورت بگیرد که به ظاهر دو مفهوم مخالف هم هستند. البته راهکارهایی نیز برای این مسائل اندیشیده شده است (مثل احراز هویت k مرتبه گمنام).

به طور کلی نیازمندی‌های حریم خصوصی در اینترنت اشیاء را می‌توان به صورت زیر دسته‌بندی کرد:

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

۲- وجود رضایت‌نامه برای استفاده از اطلاعات شخصی افراد (صدور مجوز حریم خصوصی؛ شخص باید روی افشای اطلاعات خود کنترل کامل داشته باشد)

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

۴- حفظ حریم خصوصی و گمنامی (و اجازه استفاده از نام مستعار در شرایط خاص) برای مجموعه‌های ناهمگون از دستگاه‌ها (که توسط مدیریت هویت دیجیتال مهیا می‌شود)

۵- ارائه سیاست‌ها و چارچوب لازم برای حفظ حریم خصوصی و ثبت قوانین مربوط به آن

۶- بررسی شرایط استفاده از Bridge در صورت نیاز برای حفظ حریم خصوصی

۷- سازگاری حریم خصوصی سیستم‌های مختلف

۸- حفظ حریم خصوصی در هنگام جستجو یا کشف سرویس‌ها و دستگاه‌های IoT

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

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

۱۱- تنها شخص مجاز برای خواندن برچسب‌های مرتبط با حریم خصوصی، باید مالک آن باشد

۱۲- عدم امکان ردیابی فعالیت‌های یک شیء توسط شیء دیگر

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

۱۴- ایجاد پروتکل‌ها و الگوریتم‌های مخفی کننده اطلاعات خصوصی افراد، مثل چهره یا مکان (به طوری که تنها اشخاص مجاز قابلیت باز کردن آن را داشته باشند)

۱۵- پیشنهاد پروتکل برای توافق روی سطح حریم خصوصی لازم برای اطلاعات منتشر شده

## ۵-۳- نیازمندی‌های اعتماد[۲۹۳]

مبحث اعتماد، جدای از امنیت و حریم خصوصی است. به طور کلی امنیت، تضمین کننده محرمانگی و ارسال صحیح پیام به گیرنده است، همچنین حریم خصوصی نیز تضمین می‌کند که اطلاعات حریم خصوصی کاربر تنها به اشخاص دارای مجوز منتقل شود و طبق رضایت کاربر با آن‌ها برخورد شود. اما مقوله اعتماد به معنی ایجاد تمایل برای برقراری ارتباط توسط طرفین ارتباط است. در واقع در صورتی که یک کاربر به یک فراهم کننده سرویس اعتماد داشته باشد، به اخذ سرویس از وی اقدام می‌نماید و این چیزی جز امنیت و حریم خصوصی است. در برخی شرایط حتی ممکن است که عدم وجود اعتماد به دلیل عدم آگاهی کاربر باشد که موجب جلوگیری از استفاده از سیستم و استخراج بهره از آن می‌گردد. یک سیستم غیر قابل اعتماد، به راحتی می‌تواند حریم خصوصی و امنیت کاربر را تهدید کند؛ به این ترتیب که اطلاعات رمز شده و ارسال شده به این سیستم، می‌تواند به راحتی در اختیار افراد غیر مجاز قرار گیرد، ضمن اینکه قوانین حریم خصوصی لازم الاجرا توسط این سیستم نیز نادیده گرفته شود که موجب به خطر افتادن حریم خصوصی فرد می‌شود. بنابراین ایجاد اعتماد در اینترنت اشیاء باید به صورت مجزا دیده شود که شامل نیازمندی‌های کلی زیر است:

۱- استفاده از مکانیزم‌های اعتباردهی برای شناسایی اعتبار یک سرویس‌دهنده یا نهاد
۲- بهره‌گیری از ساختار PKI سبک و امن، و استفاده از گواهی‌های دیجیتال معتبر
۳- وجود زنجیره اعتماد میان کاربران
۴- تأیید فیزیکی یک شخص یا نهاد برای برقراری ارتباط با وی یا دیگران

[۲۹۳] Trust

# ۶- چالش ها و مشکلات امنیتی (امنیت و حریم خصوصی) در اینترنت اشیا و راه حل های پیشنهادی

مهمترین چالش در اینترنت اشیاء، ارائه و پذیرش یک معماری جامع برای آن است که علاوه بر پوشش دادن مسائل ارتباطی و عملکردی، مشکلات امنیت، حریم خصوصی و اعتماد را نیز در بر بگیرد. با این حال، در این بخش ابتدا به بیان چالش‌های کلی و مسائل باز موجود در اینترنت اشیاء می‌پردازیم. سپس چالش‌های امنیتی و راه‌حل‌های پیشنهادی آن را مطرح می‌کنیم.

## ۶-۱ چالش‌های کلی و مسائل بازIoT

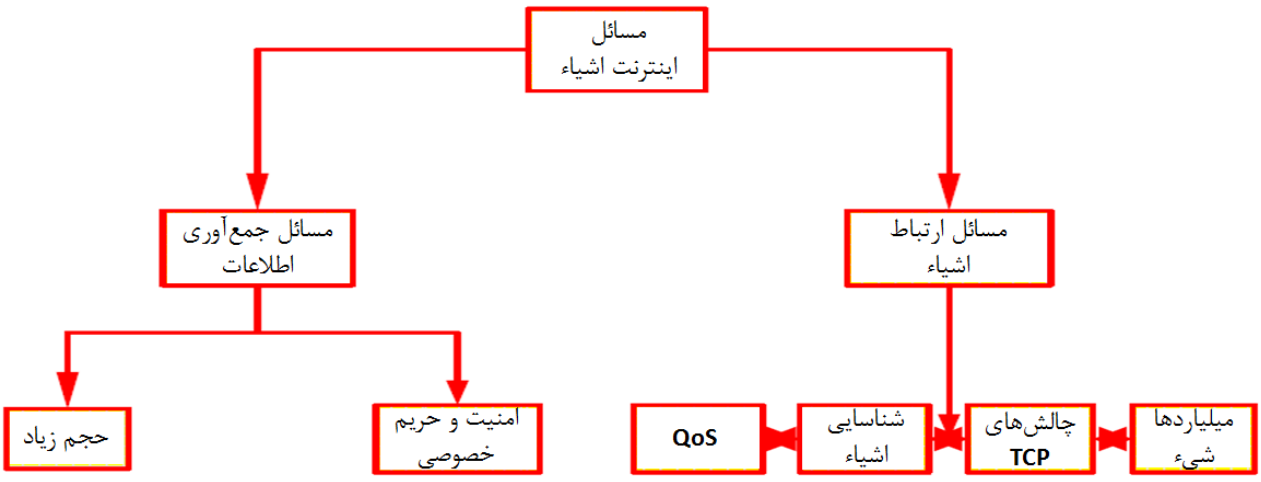
[IJCN-265]

چالش‌های متعددی برای اینترنت اشیاء وجود دارد که هنوز در مراحل تحقیقاتی قرار دارند. این چالش‌ها، مسائل بازی هستند که به دو دلیل اصلی زیر ایجاد شده‌اند:

۱- حجم انبوه اطلاعات جمع‌آوری شده برای هر شیء

۲- ارتباط میان سخت‌افزار سیستم‌ها

شکل ۶-۱-۱-۱ دسته‌بندی مشخص‌تری را از این موارد نشان می‌دهد:




شکل ۶-۱-۱-۱ دسته‌بندی چالش‌های IoT

### ۶-۱-۱- مسائل جمع‌آوری اطلاعات

مسائل این بخش می‌توانند به دو دسته اصلی تقسیم‌بندی شوند. اول به حجم زیاد اطلاعات جمع‌آوری شده به وسیله RFID اشاره دارد که از تعداد بسیار زیاد اشیاء متصل شده به سیستم IoT استخراج می‌شود. دوم بحث امنیت و حریم خصوصی اطلاعات است که به دلیل ارسال بیسیم اطلاعات باید مورد توجه قرار بگیرد.

#### ۶-۱-۱-۱- حجم زیاد اطلاعات جمع‌آوری شده

سیستم‌های IoT باید میلیاردها شیء را به یکدیگر متصل کنند و هر شیء باید اطلاعاتی را از خود منتشر کند. ایناطلاعات باید در نقطه‌ای جمع‌آوری شوند تا مورد بهره‌برداری قرار بگیرند. به دلیل تعداد بسیار زیاد اشیاء IoT، مقدار اطلاعات جمع‌آوری شده بسیار زیاد است. بنابراین، با مشکلات مختلف و زیادی در جمع‌آوری این اطلاعات مواجه خواهیم بود. از جمله این مشکلات شامل:

۱- انتقال اطلاعات: حجم بسیار اطلاعات باید به صورت آنی منتقل شوند که لزوما تضمین شده نیست. مهترین دلیل این امر نیز مربوط به محدودیت‌های پهنای باند است.

۲- ذخیره: این مسأله به دلیل حجم بالای اطلاعاتی که باید ذخیره شوند و گرفتن نسخه پشتیبان[۲۹۴] از آن‌ها مهم می‌شود.

۳- پردازش: اطلاعات جمع‌آوری شده اشیاء باید توسط کاربردهای وب پردازش و کنترل شوند تا فعالیت‌های کنترلی برای اشیاء مشخص شود. فرایند کنترل باید به صورت آنی انجام شود و نیازمند قدرت محاسباتی است.

[۲۹۴] Backup

### ۶-۱-۱-۲- امنیت و حریم خصوصی

مشخص است که داده‌ها بین اشیاء IoT به صورت بیسیم منتقل می‌شود. بنابراین امنیت و حریم خصوصی بسیار مهم می‌شود که باید به دقت بررسی شوند. در مورد امنیت، دلایل متعددی برای به خطر افتادن اطلاعات موجود در IoT وجود دارد. این دلایل شامل موارد زیر است:

۱- حملات لایه فیزیکی: یک هکر می‌تواند اطلاعات درون دستگاه‌های IoT را استخراج یا حذف کند و یا تغییر دهد، چرا که این دستگاه‌ها در اکثر اوقات در محیط رها می‌شوند.

۲- حمله به اطلاعات بیسیم:مهاجم ممکن است بتواند قبل از رسیدن اطلاعات به گیرنده، آن را بدست آورد. در این زمینه موضوعات مطالعاتی مختلف و متعددی از نظر امنیتی وجود دارد و یک چالش بزرگ محسوب می‌شود.

۳- توان دفاعی پایین: بیشتر دستگاه‌های IoT امکان پذیرش بسته‌های امنیتی را به دلایلی مثل توان مصرفی، قدرت پردازشی، هزینه و صرفه‌جویی‌های دیگر، ندارند.

حریم خصوصی یک مقوله مهم در کشورهای متمدن است. حریم خصوصی یعنی فراهم آورنده اطلاعات (یا یک کاربر) تنها توسط مشاهده استفاده از سیستم وی قابل تشخیص باشد (و حداقل، تشخیص او باید بسیار سخت باشد). جمع‌آوری، هدایت[۲۹۵] و Mining اطلاعات در سیستم‌های IoT به گونه دیگری صورت می‌گیرد و دلیل این امر، وجود راه‌حل‌های مختلف در سیستم‌های IoT است (مثل سیستم کنترل منابع خانه). بنابراین برای تضمین حریم خصوصی اطلاعات شخصی، باید از سه موضوع اصلی زیر اطمینان حاصل کنیم.

۱- چه کسی اطلاعات شخصی را جمع‌آوری می‌کند.

۲- این اطلاعات چگونه جمع‌آوری می‌شوند.

۳- زمان فرایند جمع‌آوری چه قدر است.

[۲۹۵] Handling

ضمن اینکه باید تضمین شود که اطلاعات شخصی جمع‌آوری شده توسط افراد مجاز استفاده و در سرورهای مجاز ذخیره می‌شود. همچنین هر فرد باید بداند که چه اطلاعاتی از حریم خصوصی او در اختیار افراد مجاز قرار می‌گیرد و تمام این فرایند با آگاهی، اجازه و رضایت وی انجام شود.

### ۶-۱-۲- مسائل ارتباطی اشیاء

مسائل مربوط به ارتباط بین اشیاء در IoT به دو دسته تقسیم می‌شود. دسته اول، پاسخ به مسائل اشیاء، و دسته دوم مسائل RFID در زمینه خواندن، نوشتن، و انتقال اطلاعات اشیاء است. در ادامه به بررسی مسائل ارتباطی اشیاء می‌پردازیم.

#### ۶-۱-۲-۱- میلیاردها شیء در IoT

وقتی ما به ارتباط بین تعداد زیادی از اشیاء فکر می‌کنیم، مسائل بسیاری نمایان می‌شود. از جمله این مسائل شامل موارد زیر است:

۱- سخت‌افزار چه باشد؟

۲- کدام سخت‌افزار برای ارتباط این حجم انبوه اشیاء مورد نیاز است؟

۳- روش آدرس‌دهی ایده‌آل (پروتکل) برای هر شیء در سیستم چیست؟

اگر پاسخ IPv6 باشد، سؤالات دیگری پیش می‌آید:

۱- آیا IPv6 برای آینده IoT مناسب است؟

۲- آیا سازگاری بین تعداد زیادی از سخت‌افزارها به عنوان یک فاکتور ارتباطی می‌تواند باشد یا خیر؟

همچنین، یکی دیگر از مسائل در این زمینه، نبود استاندارد است.

#### ۶-۱-۲-۲- IoT و چالش TCP

زیرساخت IoT مشابه اینترنت است. بنابراین داده‌ها از پروتکل‌های TCP و UDP برای انتقال استفاده می‌کنند. UDP یک پروتکل قابل اطمینان نیست که این کاملا خلاف هدف ماست. به همین دلیل باید TCP به عنوان پروتکل لایه انتقال سیستم‌های IoT انتخاب شود. TCP در سیستم‌های IoT دارای چالش‌های بیشتری است که از این قرارند:

۱- راه‌اندازی ارتباط: این مرحله در بسیاری از سیستم‌های IoT به دلیل انتقال اندک اطلاعات بین اشیاء در نظر گرفته نمی‌شود.

۲- کنترل ازدحام: مسأله کنترل ازدحام در سیستم‌های بیسیم (مثل سیستم‌های IoT) یک چالش محسوب می‌شود. البته در حالت انتقال اطلاعات کم بین اشیاء IoT، کنترل ازدحام نیاز نمی‌باشد.

۳- بافر کردن داده: این کار در منبع برای فرآیند بازارسال و در مقصد برای ترتیب‌دهی به فرآیند مورد نیز است. فرآیندهای بافر کردن داده برای دستگاه‌های بدون باتری مثل برچسب‌های RFID هزینه‌بر هستند.

بنابراین، UDP برای IoT مناسب نیست، و TCP نیز چالش‌های بیشتری دارد و در بسیاری از حالت‌های IoT نیاز نیست.

### ۶-۱-۲-۳-شناسایی آنی اشیاء

با تمرکز روی سیستم IoT، دو مسأله مبهم مشخص می‌شود:

۱- چگونه هر شیء تعریف شود

۲- چگونه اطلاعات هر شیء بدست آید

این مسائل با فناوری‌های RFID، EPC یا UID قابل پاسخگویی است. اما این فناوری‌ها مشکلات متعددی مثل تشعشع[۲۹۶]، حریم خصوصی، تخطی[۲۹۷] و ناسازگاری[۲۹۸] در به روز رسانی اطلاعات دارد. علاوه بر این، تعریف این فناوری‌ها برای تمام اشیاء جهان ساده نخواهد بود. یک راهکار برای پاسخ به این مسائل، استفاده از بینایی ماشین و پردازش تصویر به جای استفاده از RFID، EPC و UID است. در این راهکار، هر شیء می‌تواند مشخصات شیء دیگر را با مشاهده آن استخراج کند. مهمترین چالش این راه‌حل، کنترل آنی است. کنترل آنی یعنی ارتباط بین اشیاء سیستم IoT (مشاهده، تحلیل، و استخراج اطلاعات) باید به صورت آنی انجام پذیرد.

---

[۲۹۶] Radiation

[۲۹۷] Violation

[۲۹۸] Inconvenience

**IoTQoS-۴-۲-۱-۶**

تحقیقات در زمینه QoS به حالت‌های محدودتر مثل WSN یا RFID انجام شده است که قابل تعمیم به یک شکل جامع نیستند. همچنین به دلیل ترکیب اشیاء مختلف (با مشخصه و رفتار متفاوت) در IoT، بررسی QoS متفاوت است و نیازمند تحقیقات گسترده می‌باشد.

## ۶-۲- بررسی چالش‌ها و راه‌حل‌ها برای امنیت، حریم خصوصی و اعتماد در IoT

اینترنت اشیاء برخی چالش‌های امنیت مهمی ایجاد می‌کند که در نقشه راه نوآوری و تحقیق استراتژیک IERC 2010 نیز شناسایی شده‌اند. در اینجا به بیان جزئیات بیشتر می‌پردازیم. از آنجا که چالش‌های متعددی در امنیت، حریم خصوصی و اعتماد[۲۹۹] در IoT وجود دارد، اشتراکاتی نیز بین راه‌حل‌های آن‌ها موجود است:

- راه‌حل‌های متقارن و سبک برای پشتیبانی از دستگاه‌های با محدودیت منابع
- مقیاس‌پذیری به میلیاردها دستگاه یا تراکنش

راه‌حل‌ها باید ارتباطات و همکاری‌های اجرایی را نیز تحت پوشش قرار دهند:

- ناهمگونی[۳۰۰] و چندگانگی دستگاه‌ها و پلتفرم‌ها
- راه‌حل‌های قابل درک و استفاده که به طور بی‌درز[۳۰۱] در جهان واقعی جاسازی[۳۰۲] شده‌اند.

### ۶-۲-۱- اعتماد برای IoT

به دلیل آن که کاربردها و سرویس‌های مقیاس‌پذیر IoT روی چند دامنه اجرایی و رژیم مالکیتی گسترده شده‌اند، نیاز برای چارچوب اعتماد جهت ایجاد اعتماد بین کاربران محرز است و تبادل اطلاعات و سرویس‌ها بین کاربران وابسته به آن است. چارچوب اعتماد باید بتواند با انسان و ماشین به عنوان یک کاربر ارتباط برقرار کند، یعنی برای

---

[۲۹۹] Trust

[۳۰۰] Heterogeneity

[۳۰۱] Seamlessly

[۳۰۲] Integrated

انسان اعتماد را فراهم کند و برای ماشین به اندازه کافی مستحکم[۳۰۳] و بدون از دست دادن سرویس[۳۰۴] باشد. توسعه چارچوب‌های اعتماد به طوریکه این نیازمندی‌ها را پوشش دهد، به پیشرفت‌هایی در زمینه‌های زیر نیازمند است:

- زیرساخت کلید عمومی (PKI) سبک به عنوان یک پایه برای مدیریت اعتماد. پیشرفت‌هایی در مفاهیم گواهی‌های متقابل[۳۰۵] و سلسله‌مراتبی[۳۰۶] مورد نیاز است تا نیازهای مقیاس‌پذیری پوشش داده شود.
- سیستم‌های مدیریت کلید سبک برای ایجاد روابط اعتماد و توزیع عناصر رمزنگاری با استفاده از کمترین منابع پردازش و مخابراتی، که با طبیعت محدود شده منابع بسیاری از دستگاه‌های IoT سازگار است.
- کیفیت اطلاعات[۳۰۷] (QoI) یکی از نیازها برای بسیاری از سیستم‌های IoT است، جایی که metadata می‌تواند برای ارزیابی قابلیت اطمینان[۳۰۸] داده‌های IoT مورد استفاده قرار بگیرد.
- سیستم‌های غیرمرکزی و خودپیکربند[۳۰۹] به عنوان یک بسته اصلاحی به PKI برای ایجاد اعتماد در نظر گرفته می‌شوند (مثلا فدراسیون هویت، شخص به شخص بودن)
- روش‌های جدید ارزیابی اعتماد در مردم، دستگاه‌ها و داده‌ها در ورای سیستم‌های اعتباری. یک مثال از این دست، مذاکره اعتماد[۳۱۰] است. مذاکره اعتماد مکانیزمی است که به دو فرد اجازه می‌دهد تا به صورت اتوماتیک بر اساس یک زنجیره سیاست‌های اعتماد مذاکره کنند. این مکانیزم، کمترین سطح اعتماد مورد نیاز برای دسترسی رسمی به یک سرویس یا اطلاعات را فراهم می‌کند.
- روش‌های اعتماد[۳۱۱] برای پلتفرم‌های مورد اعتماد شامل سخت‌افزار، نرم‌افزار و پروتکل‌ها.

---

[۳۰۳] Robust

[۳۰۴] Denial of Service

[۳۰۵] Cross Certification

[۳۰۶] Hierarchical

[۳۰۷] Quality of Information

[۳۰۸] Reliability

[۳۰۹] Self-configure

[۳۱۰] Trust Negotation

[۳۱۱] Assurance

- کنترل دسترسی برای جلوگیری از نفوذ به داده‌ها[۳۱۲]. یک مثال برای این قسمت، کنترل استفاده [۳۱۳] است که فرآیند تضمین استفاده صحیح از اطلاعات خاص بر طبق سیاست‌های از پیش تعیین شده بعد از اجازه دسترسی به آن اطلاعات است.

### ۶-۲-۲- امنیت برای IoT

به دلیل آنکه IoT یک عنصر کلیدی اینترنت آینده و زیرساخت ملی/بین‌المللی بحرانی است، ایجاد امنیت کافی برای زیرساخت IoT بسیار اهمیت پیدا می‌کند. کاربردهای IoT از حسگرها و محرک‌های فشرده شده در محیط استفاده می‌کند و آن‌ها حجم زیادی از داده‌ها را در مورد دما، رطوبت و نور برای بهینه کردن مصرف انرژی جمع‌آوری می‌کنند و از خطای عملیاتی که تأثیر واقعی بر محیط دارد، دوری می‌کنند. در صنعت خرده‌فروشی[۳۱۴]، یخچالی که نتواند در دمای مناسب (و به اندازه کافی پایین) باقی بماند، ممکن است داروها و غذاهای گران قیمت را در معرض ریسک قرار دهد. با داشتن همه این دستگاه‌های متصل شده به هم، تنها نیاز است که مدل داده[۳۱۵] درست را داشته باشیم. مدل داده باید داده حسگر با ریت بالا را در خود جا دهد تا اطلاعات را جذب و تحلیل نماید. در این پایگاه داده مفهومی، عملکرد خواندن و نوشتن بسیار مهم است، به ویژه وقتی ریت داده بالا باشد. این پایگاه داده باید خواندن و نوشتن‌های با سرعت بالا را پشتیبانی کند و به طور مداوم در دسترس باشد (۱۰۰٪ زمان‌ها) تا این اطلاعات را در دوره‌های یکنواخت جمع‌آوری کند و مقیاس‌پذیر باشد تا کارایی هزینه را برای ذخیره داده‌ها در زمان حفظ نماید.

سرویس‌ها و کاربردهای مقیاس بزرگ بر اساس IoT، به طور مستمر توسط اغتشاشات حمله یا دزدی اطلاعات تهدید می‌شوند. پیشرفت‌های متعددی در زمینه‌های مختلف احتیاج است تا IoT را در برابر این مقاصد مختصمانه محافظت کند که شامل موارد زیر هستند:

---

[۳۱۲] Data breach

[۳۱۳] Usage Control

[۳۱۴] Retail

[۳۱۵] Data model

- حملات DoS/DDoS برای اینترنت فعلی کاملا مطالعه شده‌اند، اما IoT هنوز در برابر چنین حملاتی حساس است و روش‌ها و مکانیزم‌های خاصی برای اطمینان از عدم غیرفعال‌سازی یا واژگونی زیرساخت‌های حمل و نقلی، انرژی و شهری احتیاج است.
- شناسایی کلی حملات و بازیابی/مقاومت برای مقابله با تهدیدات خاص IoT مثل گره‌های مصالحه شده و حملات هک کد بدخواه.
- روش‌ها و ابزارهای آگاهی از شرایط سایبری باید توسعه پیدا کنند تا زیرساخت‌های متکی به IoT قابلیت نظارت شدن را داشته باشند. پیشرفت‌هایی برای توانمندسازی اپراتور برای وفق دادن محافظت از IoT در حین چرخه عمر سیستم، و برای اپراتورهای کمکی جهت انجام بیشترین واکنش حفاظتی مناسب در خلال حملات نیاز است.
- IoT به تنوعی از طرح‌های کنترل دسترسی و حسابرسی وابسته نیاز دارد تا از صدور مجوزها و مدل‌های استفاده مختلف مورد نیاز برای کاربر، پشتیبانی نماید. ناهمگونی و گوناگونی[۳۱۶] دستگاه‌ها/درگاه‌های[۳۱۷] مورد نیاز کنترل دسترسی، به طرح‌های سبک جدیدی برای توسعه احتیاج دارد. IoT نیاز دارد تا به طور مجازی، همه سبک‌های عملیاتی[۳۱۸] را توسط خودش و بدون وابستگی به کنترل انسانی، هدایت نماید. رویکردها و روش‌های جدیدی مثل یادگیری ماشین، برای هدایت به سوی IoT خودمدیریتی[۳۱۹] مورد نیاز است.

---

[۳۱۶] Diversity

[۳۱۷] Gateway

[۳۱۸] Modes of Operation

[۳۱۹] Self-managed IoT

### ۶-۲-۳- حریم خصوصی برای IoT

از آنجایی که بسیاری از اطلاعات در سیستم IoT ممکن است اطلاعات شخصی باشد، نیاز به پشتیبانی از گمنامی و کنترل محدود شده اطلاعات شخصی وجود دارد. در اینجا تعدادی از موضوعات حریم خصوصی که باید توسعه یابند، مطرح می‌شود:

- روش‌های رمزنگاری که امکان ذخیره‌سازی، پردازش و به اشتراک گذاری داده‌های حفاظت شده را بدون در دسترس قرار دادن محتویات به دیگر بخش‌ها، ایجاد می‌کند. فناوری‌هایی مثل رمزنگاری هومومورفیک و قابل جستجو، یک کاندید مناسب برای توسعه این موارد هستند.
- روش‌هایی برای پشتیبانی از مفاهیم حریم خصوصی به وسیله طراحی[۳۲۰]، شامل کمینه‌سازی داده[۳۲۱]، شناسایی، احراز اصالت و گمنامی
- مکانیزم کنترل دسترسی خود پیکربند و Fine-grain که از جهان واقعی تقلید می‌کند.

همچنین تعدادی مفاهیم حریم خصوصی وجود دارد که از فراگیر بودن دستگاه‌های IoT ناشی می‌شوند و تحقیقات بیشتر احتیاج دارند:

- حفظ حریم خصوصی مکانی[۳۲۲]؛ مکان می‌تواند از اشیاء وابسته به مردم حدس زده شود.
- جلوگیری از استنتاج اطلاعات شخص؛ هر فرد می‌خواهد اطلاعات شخصی وی در مشاهده تبادلات مرتبط با IoT، منتشر نشود.
- نگهداری محلی اطلاعات تا حد ممکن، با استفاده از محاسبات غیرمرکزی و مدیریت کلید.
- استفاده از هویت‌های نرم؛ هویت واقعی یک کاربر می‌تواند برای تولید هویت‌های نرم مختلف برای کاربردهای خاص مورد استفاده قرار بگیرد. هر هویت نرم می‌تواند برای یک موضوع یا کاربرد خاص طراحی شود، بدون آنکه اطلاعاتی که سبب از بین رفتن حریم خصوصی می‌شود، منتشر شوند.

---

[۳۲۰] Privacy by Design

[۳۲۱] Data minimization

[۳۲۲] Location Privacy

### ۶-۲-۴- چالش‌های امنیتی IoT از نگاه کتاب Zhou

در IoT، به دلیل آنکه بسیاری از اشیاء (دستگاه‌ها، سرمایه‌ها، تجهیزات، تسهیلات و غیره) تحت مالکیت نهادهای مشخصی هستند، مشخصه‌های مالکیت مبحث امنیت سیستم‌های IoT را بسیار مهم‌تر، و پیچیده‌تر از امنیت سیستم‌های ICT می‌کند. همچنین، حریم خصوصی مثل مکان جغرافیایی یک شخص یا شیء نیز یکی از مهمترین نگرانی‌های امنیتی در IoT است. شکی وجود ندارد که IoT، چالش‌های امنیتی جدیدی را در امنیت، صدور اعتبارنامه و مدیریت هویت ایجاد می‌نماید.

با این حال، تفاوت بنیادین بین امنیت IoT و امنیت سیستم‌های ICT وجود ندارد. امنیت سیستم‌های ICT جدید دارای ۸ بعد است: کنترل دسترسی، احراز هویت، انکارناپذیری، محرمانگی داده، امنیت مخابره، یکپارچگی داده، دسترس‌پذیری، و حریم خصوصی. این موارد باید در سیستم‌های IoT نیز به کار گرفته شوند و می‌توانند بیشتر نگرانی‌های امنیتی IoT را پوشش دهند (البته لزومی ندارد که همه نگرانی‌ها را پوشش دهند).

برخی موضوعات خاص امنیتی که بیشتر در سناریوهای کاربرد IoT دیده می‌شوند، شامل موارد زیر است:

- Skimming: داده‌ها بدون مشخص بودن دانش Tag یا دارنده آن، مستقیما از روی Tag خوانده می‌شوند.
- استراق سمع (Eavesdropping یا Sniffing؛ یا مرد در میانه نیز اتلاق می‌شود): گوش دادن و حائل شدن بدون مجوز
- Data Tampering: پاک کردن بدون مجوز داده‌ها برای بی‌استفاده کردن دستگاه یا تغییر اطلاعات آن
- Spoofing: کپی کردن داده‌های دستگاه و انتقال آن به گیرنده برای جعل کردن آن
- Cloning: کپی کردن داده‌های یک دستگاه در دیگری
- کد بدخواه (Malicious Code): اضافه کردن یک کد قابل اجرا (مثل ویروس) برای تخریب سیستم
- رد دسترسی یا سرویس (Denial of Access/Service): وقتی اتفاق می‌افتد که چند دستگاه برای مصرف کل ظرفیت گیرنده مورد استفاده قرار می‌گیرند که سبب می‌شود تا سیستم غیر فعال شود.
- کشتن (Killing): تخریب فیزیکی یا الکترونیکی یک دستگاه که سبب بی‌بهره شدن کاربران استفاده کننده از آن می‌شود.

- اختلال (Jamming): استفاده از دستگاه‌های الکترونیکی که سبب تخریب توابع گیرنده بشود.
- سپر گذاری (Shielding): استفاده از ابزارهای مکانیکی برای جلوگیری کردن از خواندن یک Tag یا دستگاه

در هنگام توسعه و طراحی امنیت IoT، علاوه بر چالش‌های امنیتی ICT، باید موارد فوق را نیز در نظر گرفت:

- ۱۰ موضوع امنیتی که در بالا مطرح شده به همراه تعداد دستگاه‌هایی که مشارکت می‌کنند، طراحی و توسعه راه‌حل‌های امنیتی را پیچیده‌تر می‌کند.
- محیط شبکه‌ای ناهمگون، چند هاب و توزیع شده، عبور و ترجمه اعتبارنامه‌های امنیتی و توابع امنیت پایان به پایان را در چهار دسته شبکه موجود (شبکه بیسیم یا سیمی برد کوتاه یا بلند) بسیار پیچیده می‌کند.
- اولیه‌های رمزنگاری با این فرض طراحی شده‌اند که منابع کافی مثل سرعت پردازش و حافظه) برای آن‌ها در دسترس است. تغییر اندازه‌ها، ظرفیت حافظه محدود، و قدرت پردازشی محدود یک دستگاه، پردازش‌های مربوط به رمزنگاری، رمزگشائی، امضا و مدیریت کلید زیرساخت کلید عمومی (PKI) را با مشکل مواجه می‌کند، ضمن اینکه موجب نشت اطلاعات نیز می‌شود.
- وارد شدن و خارج شدن دستگاه‌ها (bootstrapping) در یک سیستم IoT و گروه شدن دستگاه‌های موبایل در یک شبکه داینامیک نیز موجب پیچیده‌تر شدن فرایندهای احراز هویت و صدور مجوز می‌شود.
- به عنوان راهکار کاندید، پروتکل‌های زیر در تیم‌های CoRE IETF و 6LoWPAN پیشنهاد شده است:
- تبادیل کلید اینترنت IPsec/(IKEv2) و MOBIKE (IKEv2) که به آن Multi-homing و تحرک نیز اضافه شده است)
- پروتکل شناسایی مهمان[۳۲۳] (HIP) و نسخه‌ای از آن برای شبکه‌های کم‌توان اتلاف‌گر که به آن Diet HIP گفته می‌شود.

[۳۲۳] Host Identity Protocol

- امنیت لایه انتقال (TLS) و نسخه Datagram آن (DTLS) که ارتباطات لایه انتقال را امن می‌کند.
- پروتکل احراز هویت توسعه‌پذیر[۳۲۴] (EAP)
- پروتکل ایجاد احراز هویت برای دسترسی به شبکه[۳۲۵] (PANA)

همچنین SMEPP[۳۲۶] نیز یک پروژه است که یک چارچوب میان‌افزار امنیت برای کاربردهای IoT ایجاد می‌کند.

[۳۲۴] Extensible Authentication Protocol

[۳۲۵] Protocol for Carrying Authentication for Network Access

[۳۲۶] Secure Middleware for Embedded Peer-to-Peer

# ۷- معرفی معماری‌های مطرح شده برای اینترنت اشیاء

در این بخش، معماری‌های کلان مطرح شده در زمینه اینترنت اشیاء بررسی می‌گردد.

## ۷-۱- معماری ARM[۳۲۷]

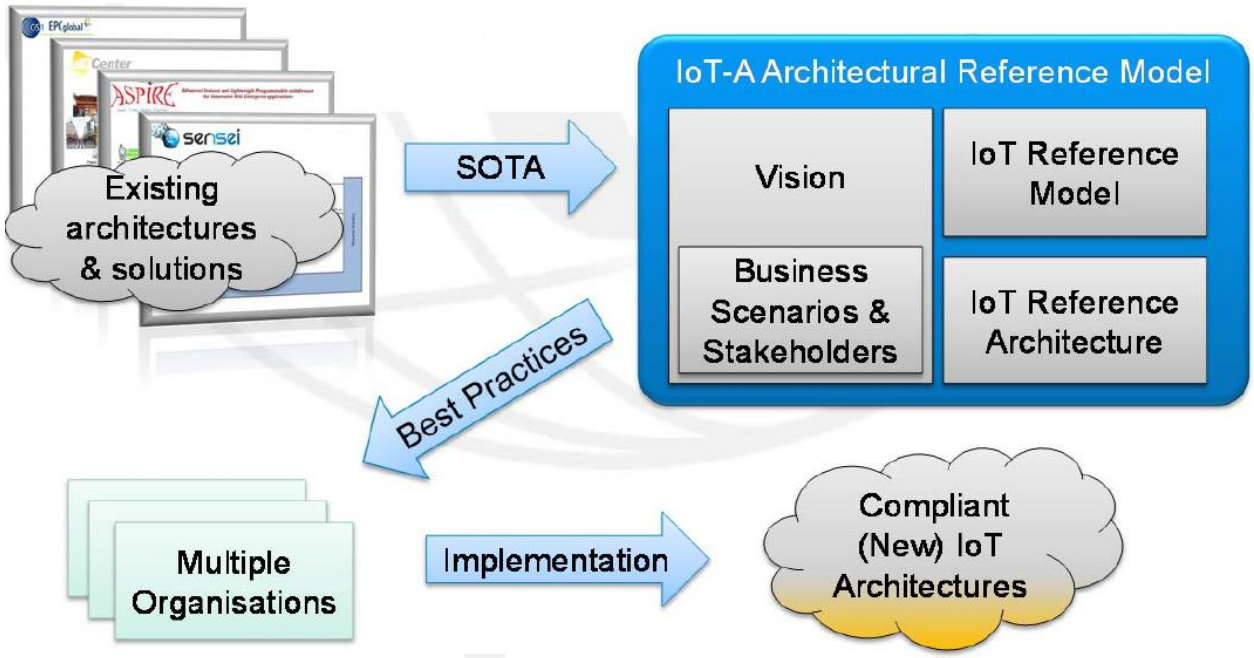
این معماری، خروجی پروژه IoT-A در مرکز تحقیقات بین‌المللی اتحادیه اروپا است که هم‌اکنون، آخرین نسخه آن (ARM v2) در گزارش D1.4 پروژه در دسترس است. سرچشمه نیاز به یک معماری جامع برای اینترنت اشیاء، مبحث سازگاری است. در دنیای حاضر، شبکه‌های هوشمند مختلفی طراحی شده است که هر کدام برپایه معماری خاص خود پیاده‌سازی شده و سازگار با دیگری نمی‌باشد. در واقع این شبکه‌های هوشمند، زیر مجموعه‌های بزرگ، اما مجزا از اینترنت اشیاء هستند که در واقع به جای هدف اصلی خود، اینترانت اشیاء را تشکیل داده‌اند. برای رسیدن به هدف اصلی، نیاز به یک معماری جامع برای پیاده‌سازی اینترنت اشیاء هست تا این شبکه‌های مختلف، بر اساس یک بستر یکسان (مشابه درختی با برگ‌های مختلف، اما تنه یکتا؛ شکل ۷-۱-۱-۱) اجرایی شوند و بتوانند ضمن ایجاد سازگاری با یکدیگر، از همدیگر پشتیبانی کنند و با یکدیگر ارتباط برقرار نمایند. به همین دلیل نیز IoT-A اجرایی شد تا یک معماری مرجع (ARM) برای اینترنت اشیاء ارائه دهد.

معماری ARM می‌تواند به صورت یک ماتریس دیده شود که نقطه شروع ایده‌آل همه معماری‌ها از آن سرچشمه می‌گیرد. برای ارائه چنین ماتریسی، باید همه مکانیزم‌ها، وظایف و پروتکل‌های قابل استفاده برای ساختن آن مشخص شوند و نحوه ایجاد ارتباط میان آن‌ها نیز بیان شود. اگرچه هیچ سیستمی، تمامی این موارد را به یکباره استفاده نخواهد کرد، اما معماری جامعی مثل ARM باید تمامی این موارد را پوشش دهد. بنابراین یک طراح سیستم، معماری مورد استفاده خود را با انتخاب از پروتکل‌ها، اجزای عملیاتی و سایر موارد موجود در معماری جامع تعیین می‌کند. در واقع با توجه به شکل ۷-۱-۱-۱، معمار طبق کاربردهای مورد نظر خود، پروتکل‌های ارتباطی و فناوری‌های موجود را برای سیستم خود انتخاب می‌کند.

[۳۲۷] Architectural Reference Model


شکل ۷-۱-۱-۱ درخت معماری ARM

ARM ترکیبی از مدل مرجع و معماری مرجع، شامل مجموعه مدل‌ها، راهنماها، بهترین تجربه‌ها، دیدگاه‌ها و جنبه‌های قابل استفاده برای ساختن سیستم‌ها و معماری IoT سازگار است. ARM شامل چهار بخش زیر است (شکل ۷-۱-۱-۲):



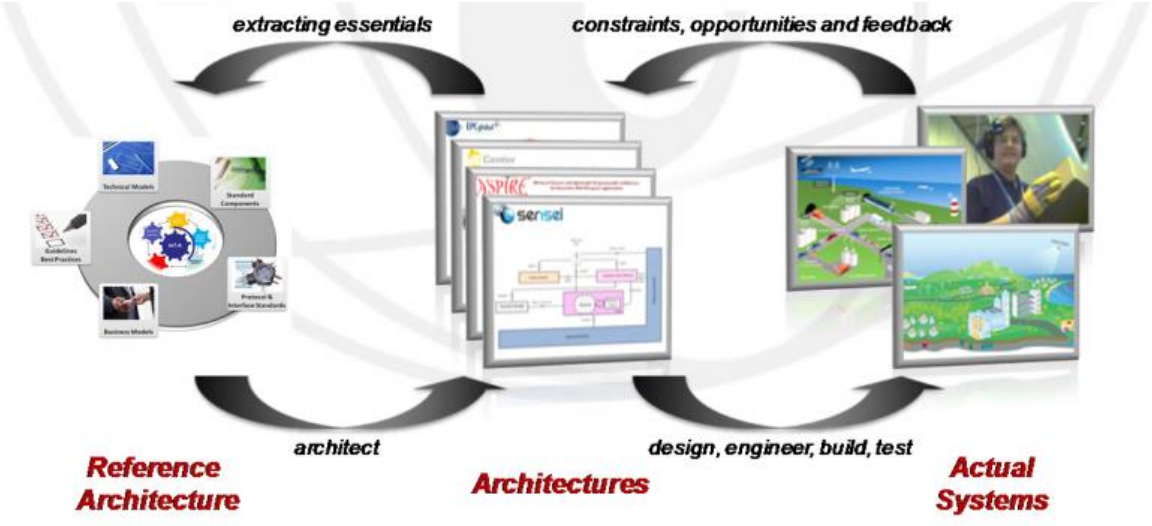

شکل ۷-۱-۱-۲ اجزای سازنده ARM

- خلاصه چشم‌اندازها که منطق مورد نیاز برای ایجاد یک مدل مرجع معماری برای IoT را ارائه می‌دهد و به طور همزمان، فرضیات موجود مثل انگیزه‌ها را نیز بیان می‌کند. همچنین، نحوه استفاده از ARM، متدولوژی آن، سناریوهای تجاری و ذی‌النفعان را نیز مشخص می‌نماید.
- سناریوهای تجاری به عنوان یک نیازمندی ذی‌النفعان تعریف می‌شوند و پیشران‌های کار هستند. با آگاهی بر تنفس‌های تجاری، نگاه کل‌نگرانه معماری‌های IoT قابل استخراج است. علاوه بر این، یک نمونه معماری مرجع می‌تواند در مقابل سناریوهای تجاری ارزیابی شود. یک تحلیل ذی‌النفعانه می‌خواهد بداند که چه جنبه‌هایی از ARM نیاز به توصیف برای ذی‌النفعان و رفع نگرانی آن‌ها دارد. به دلیل استفاده مشترک، این بخش زیر مجموعه چشم‌اندازها در نظر گرفته می‌شود.
- مدل مرجع IoT بیشترین سطح چکیده‌سازی را برای تعریف ARM ارائه می‌دهد و یک فهم مشترک از دامنه IoT ایجاد می‌کند. توصیف مدل مرجع IoT شامل کلیه دامنه‌های IoT، یک مدل دامنه به

عنوان توصیف بالا، یک مدل اطلاعاتی IoT شرح دهنده چگونگی مدل‌شدن اطلاعات IoT، و یک مدل ارتباطی IoT به منظور درک ویژگی‌های ارتباطی بین دستگاه‌های ناهمگون و اینترنت به طور کلی، است. تعریف مدل مرجع IoT بر تعریف مدل مرجع OASIS منطبق است.

- معماری مرجع IoT، یک مرجع مناسب برای ساختن معماری IoT است. این معماری، دیدگاه‌ها و جنبه‌های مختلف را برای ذی‌النفعان IoT در نظر می‌گیرد. ایجاد معماری مرجع IoT، بیشتر روی مجموعه‌های چکیده مکانیزم‌ها تمرکز دارد تا معماری‌های کاربرد.

برای سازمان‌ها، یکی از مهمترین جنبه‌ها، برآوردن فناوری‌ها با استانداردها و تجربیات است که به وسیله آن سازگاری در میان آن‌ها تضمین می‌شود (که IoT-A ARM نیز همین کار را می‌کند). شکل ۷-۱-۱-۳ نحوه اقتباس از معماری مرجع و استفاده از آن برای ساخت یک معماری و در نهایت سیستم‌ها در اینترنت اشیاء را برای سازمان نوعی به طور مفهومی نشان می‌دهد.



شکل ۷-۱-۱-۳ نحوه اقتباس از معماری مرجع و ساخت معماری و سیستم‌ها در اینترنت اشیاء بر اساس مدل IoT-A

### ۷-۱-۲- فواید استفاده از ARM

این فواید شامل موارد زیر است:

۱- کمک‌های شناختی:

I. از آنجا که یک زبان همگانی ارائه می‌دهد، به مباحث راهنمایی کمک می‌کند و آن‌ها را به معماری، سیستم و دامنه استفاده متصل می‌کند.

II. نگاه سطح بالای موجود در این مدل دارای ارزش علمی بالایی است. اگر چه این نگاه یک چکیده ایجاد می‌کند، اما نگاه دامنه را پربار می‌نماید. چنین نگاهی می‌تواند به تازه‌کاران کمک کند تا ویژگی‌ها و پیچیدگی‌های IoT را درک نمایند.

III. ARM می‌تواند به رهبران پروژه‌های IoT در برنامه‌ریزی کارها و نیازهای تیمی کمک کند. برای مثال، گروه وظایف شناسایی شده در نگاه وظیفه‌محور سیستم IoT می‌تواند به عنوان یک لیست تیم‌های مستقل که روی پیاده‌سازی یک سیستم IoT کار می‌کنند، در نظر گرفته شود.

IV. ARM در شناسایی اجزای سازنده مستقل برای سیستم‌های IoT نیز مؤثر است. این تأثیر اطلاعات بسیار با ارزشی را تشکیل می‌دهد که برای پاسخ به سوالاتی مثل پیمانه‌ای بودن سیستم[۳۲۸]، معماری پردازنده، انتخاب‌های فروشنده سوم، باز استفاده از اجزای ایجاد شده و غیره مفید است.

۲- مدل مرجع IoT-A به عنوان زمین مشترک[۳۲۹]: ایجاد یک زمین مشترک برای یک حوزه، کار ساده‌ای نیست. برای کارا بودن، این زمین باید تا جای ممکن فرصت‌های مناسب را در اختیار بگیرد. ایجاد یک زمین مشترک باید تعریف نهادهای IoT را در بر بگیرد و تراکنش‌ها و ارتباطات پایه آن‌ها را با یکدیگر توصیف کند. ARM دقیقا چنین زمین مشترکی را برای حوزه IoT ایجاد می‌کند. هر بخشی که با توسعه

[۳۲۸] System Modularity

[۳۲۹] Common Ground

یک سیستم IoT که منطبق با IoT-A است، مواجه می‌شود، باید مفاهیم مشترکی که در مدل مرجع IoT-A وجود دارد را بسازد.

۳- ایجاد معماری‌ها: یکی دیگر از این فواید، استفاده از ARM برای ایجاد معماری‌های مناسب برای سیستم‌های خاص است. این کار با فعال کردن پشتیبان ابزار[۳۳۰] قابل انجام است. فایده چنین طرح تولیدی برای معماری IoT، نه تنها در اتوماسیون این فرآیند، و لذا در کاهش هزینه‌های R$D است، بلکه معماری ساخته شده یک سازگاری ذاتی برای سیستم‌های IoT مشتق شده ایجاد می‌نماید.

۴- شناسایی تفاوت‌ها: وقتی که از ابزار تولید سیستم فوق استفاده می‌کنیم (که بر اساس ARM است)، هر تغییر در معماری مشتق شده می‌تواند به ویژگی‌های مناسب موقعیت استفاده، نسبت داده شود. وقتی IoT-A ARM به کار گرفته می‌شود، پیش‌بینی پیچیدگی سیستم (و موارد دیگر) برای بخش‌های سیستم به جهت پیاده‌سازی در دسترس است. لذا کل تلاش لازم برای پیاده‌سازی در این حالت آسان‌تر است و برخی پروژه‌ها که به دلیل برخی عدم قطعیت‌ها ممکن است عملی به نظر نرسند، امکان‌پذیر می‌شوند. پیاده‌سازی کلی بسیار کمتر از ایجاد یک معماری بدون کمک گرفتن از ARMهزینه در بر دارد.

۵- محک زدن[۳۳۱]: اگرچه مدل مرجع زبان مورد استفاده در سیستم/معماری را تعیین می‌کند تا ارزیابی شود، اما معماری مرجع کمترین نیاز برای سیستم/معماری را بیان می‌کند. همچنین معماری مرجع به وسیله استاندارد کردن توصیف و همچنین مرتب‌سازی و توصیف جنبه‌ها و اجزای سیستم، سطح بالایی از شفافیت و مقایسه‌پذیری ذاتی را برای فرایند محک زنی ایجاد می‌کند.

---

[۳۳۰] Tool Support

[۳۳۱] Benchmarking

### ۷-۱-۳- امنیت در معماری ARM

در این بخش، ویژگی‌های اساسی سیستم‌های IoT در زمینه اعتماد، امنیت، حریم خصوصی و دسترس‌پذیری از دیدگاه معماری ARM (پروژه IoT-A) مطرح می‌شود. این سه زمینه به یکدیگر مرتبطند و معمولا، تکامل یا بهبود یکی از آن‌ها وابسته به همین تکامل و بهبود در دوتای دیگر است.

#### ۷-۱-۳-۱-اعتماد

اعتماد در محیط IoT بسیار اساسی است، اگرچه بدست آوردن آن بسیار مشکل است. همانند امنیت، این ویژگی نیز بسیار وابسته به عملکرد محاسباتی و ارتباطی سیستم است. در چارچوب IoT، نهادهای M2M باید امکان ارزیابی اعتماد را به منظور رسیدن به سیستم‌های مستقل فراهم کنند. جنبه‌های اعتماد در IoT در جدول ۷-۱-۳-۱ آمده است.

**جدول ۷-۱-۳-۱ جنبه‌های اعتماد در IoT**

| | |
|---|---|
| ویژگی مورد انتظار | یک ویژگی پیچیده مرتبط با قابلیت اعتماد که یک نهاد (به صورت معقولانه) از سیستم IoT در مورد همه جنبه‌های رفتاری آن انتظار دارد. |
| نیازمندی‌های IoT-A | کدهای شناسایی نیازمندی‌های اعتماد در پروژه IoT-A شامل موارد زیر است. با مراجعه به این کدها در نیازمندی‌های اعتماد پروژه IoT-A، می‌توان جزئیات آن‌ها را مشاهده کرد.<br>UNI.062, UNI.065, UNI.099, UNI.407, UNI.408, UNI.602, UNI.604, UNI.605, UNI.620, UNI.622 |
| کارایی | مرتبط با سیستم‌هایی که استفاده از منابع را بین نهادهایی که از پیش مورد اعتماد نیستند، به اشتراک می‌گذارد. |
| فعالیت‌ها | ۱- استخراج نیازمندی‌های اعتماد<br>۲- انجام تحلیل ریسک<br>۳- بررسی نیازهای سازگاری و تأثیر آن روی اعتماد بین نهادهای ناهمگون<br>۴- تعریف مدل اعتماد |

| | |
|---|---|
| راهبردها | ۱- سخت کردن[۳۳۲] ریشه اعتماد<br>۲- اطمینان از امنیت فیزیکی و اجرایی کردن شناسایی نفوذ[۳۳۳]<br>۳- بررسی و تضمین تازگی داده‌ها<br>۴- در نظر گرفتن اثر بینابینی امنیت و عملکرد در اعتماد<br>۵- دوری از تغییر عقیده[۳۳۴]<br>۶- استفاده از سازمان‌های با زیرساخت معتبر و معتمد برای مقیاس‌پذیری<br>۷- استفاده از مهر امنیتی[۳۳۵] |

### ۷-۱-۳-۲- امنیت

امنیت یکی از ضروری‌ترین ویژگی‌های یک سیستم IoT است و به طور خاص به ویژگی‌های امنیتی بستگی دارد که معمولا پیشنیاز ایجاد اعتماد و حریم‌خصوصی در یک سیستم هستند. جنبه‌های امنیتی IoT در جدول ۷-۱-۳-۱ آمده است.

**جدول ۷-۱-۳-۱ جنبه‌های امنیتی IoT**

| | |
|---|---|
| ویژگی مورد انتظار | توانایی سیستم برای ایجاد سیاست‌های محرمانگی، یکپارچگی و دسترس‌پذیری به سرویس، و شناسایی و استخراج اشتباهات در این مکانیزم‌های امنیتی |
| نیازمندی‌های IoT-A | کدهای شناسایی نیازمندی‌های امنیتی در پروژه IoT-A شامل موارد زیر است. با مراجعه به این کدها در نیازمندی‌های امنیتی پروژه IoT-A، می‌توان جزئیات آن‌ها را مشاهده کرد.<br>UNI.062, UNI.407, UNI.408, UNI.410, UNI.412, UNI.413, UNI.424, UNI.502, UNI.507, UNI.604, UNI.609, UNI.611, UNI.612, UNI.617, UNI.618, UNI.624, UNI.719 |

[۳۳۲] Harden

[۳۳۳] Tampering

[۳۳۴] Leap of Faith

[۳۳۵] Security Imprinting

| کارایی | مرتبط با تمام سیستم‌های IoT |
|---|---|
| فعالیت‌ها | ۱- استخراج نیازمندی‌های امنیتی<br>۲- بررسی نیازمندی‌های سازگاری برای تأثیر در فرایندهای امنیتی میان اعضای ناهمگون<br>۳- هدایت تحلیل ریسک<br>۴- استفاده از اجزای زیرساختی[۳۳۶] احراز هویت که از چارچوب‌های شناسایی بیشتری به منظور سازگاری و مقیاس‌پذیری پشتیبانی کنند.<br>۵- استفاده از KEM[۳۳۷] فدرال یا زیرساختی برای آغاز ارتباط امن و ایجاد تونل بین درگاه‌ها برای سازگاری<br>۶- استفاده از یک بخش صدور مجوز برای ایجاد سازگاری با دیگر سیستم‌ها<br>۷- تعریف اثرات امنیتی روی مدل‌های تراکنش<br>۸- پاسخ به همه جنبه‌های امنیت ارتباط و سرویس<br>۹- جاسازی مدل اعتماد و پشتیبانی از ویژگی‌های حریم خصوصی<br>۱۰- شناسایی نیازمندی‌های سخت‌افزاری امنیت<br>۱۱- در نظر گرفتن بینابینی موجود میان امنیت و عملکرد<br>۱۲- قانونی کردن[۳۳۸] نیازمندی‌ها |
| راهبردها | ۱- سخت کردن اجزای زیرساختی کاربردی<br>۲- احراز هویت نهادها<br>۳- تعریف و اجبار سیاست‌های دسترسی<br>۴- زیرساخت ارتباطی امن (درگاه‌ها، سرویس‌های زیرساخت)<br>۵- ارتباط امن بین اشیاء<br>۶- شبکه‌های جانبی امن (امنیت لایه پیوند، ورودی شبکه، مسیریابی امن، تحرک‌پذیری و Handover)<br>۷- دوری از ارتباط بی‌سیم در هر جا که امکان‌پذیر است<br>۸- دستگاه‌های جانبی حفاظت شده به صورت فیزیکی<br>۹- دوری از مدیریت دستگاه OTA[۳۳۹]؛ اگر واجب است، امن‌سازی شود |

[۳۳۶] Infrastructural

[۳۳۷] Key Exchange Mechanism

[۳۳۸] Validate Against

[۳۳۹] Over The Air

### ۷-۱-۳-۳- حریم خصوصی

معمولا مفاهیم مختلفی با بحث حریم خصوصی منتقل می‌شود که بدون فراموش شدن جنبه‌های اخلاقی، برخی بیش از جنبه فنی مسائل هستند و برخی بیش از جنبه‌های قانونی. در جدول ۷-۱-۳-۱، جنبه‌های حریم خصوصی در IoT آمده است.

**جدول ۷-۱-۳-۱ جنبه‌های حریم خصوصی در IoT**

| ویژگی مورد انتظار | - |
|---|---|
| نیازمندی‌های IoT-A | کدهای شناسایی نیازمندی‌های حریم خصوصی در پروژه IoT-A شامل موارد زیر است.<br>با مراجعه به این کدها در نیازمندی‌های حریم خصوصی پروژه IoT-A، می‌توان جزئیات آن‌ها را مشاهده کرد.<br>UNI.001, UNI.002, UNI.410, UNI.412, UNI.413, UNI.424, UNI.501, UNI.606, UNI.611, UNI.623, UNI.624 |
| کارایی | مرتبط با همه سیستم‌ها |
| فعالیت‌ها | ۱- استخراج نیازمندی‌های حریم خصوصی<br>۲- هدایت تحلیل ریسک<br>۳- ارزیابی پذیرش[۳۴۰] با چارچوب‌های حریم خصوصی موجود |
| راهبردها | ۱- استفاده از مدیریت هویتی که اسم مستعار را نیز پشتیبانی کند<br>۲- دوری از ارسال شناساگرهایی به صورت غیر رمز شده، مخصوصا در اتصالات بی‌سیم |

[۳۴۰] Compliancy

| | |
|---|---|
| | ۳- کمینه کردن دسترسی بدون مجوز به اطلاعات مطلق[۳۴۱] (مثل استخراج اطلاعات مکان از درخواست‌های دسترسی به سرویس)<br>۴- قانونی کردن نیازمندی‌ها<br>۵- در نظر گرفتن اثر بینابینی میان امنیت و عملکرد در حریم خصوصی<br>۶- توانمندسازی کاربر برای کنترل تنظیمات حریم خصوصی خود (و بنابراین امنیت و اعتماد خود)<br>۷- تعادل میان حریم خصوصی و انکارناپذیری[۳۴۲] (قابلیت حسابرسی[۳۴۳]) |

### ۷-۱-۳-۴- دسترس‌پذیری

از آنجا که ما با سیستم‌های IoT توزیع شده سر و کار داریم، یعنی جایی که احتمال دارد اشیاء مختلف دچار خرابی[۳۴۴] شوند، توانایی سیستم برای عملیاتی ماندن و هدایت کارای خرابی‌ها که می‌تواند روی دسترس‌پذیری آن تأثیر بگذارد، بسیار حیاتی است. جنبه‌های مرتبط با دسترس‌پذیری سیستم‌های IoT در جدول ۷-۱-۳-۱ آمده است.

**جدول ۷-۱-۳-۱ جنبه‌های مرتبط با دسترس‌پذیری سیستم‌های IoT**

| | |
|---|---|
| ویژگی مورد انتظار | توانایی سیستم برای کاملا یا به طور جزئی عملیاتی ماندن در زمانی که احتیاج است، و هدایت کارای خرابی‌هایی که می‌توانند دسترس‌پذیری سیستم را تحت الشعاع قرار دهند. |
| نیازمندی‌های IoT-A | کدهای شناسایی نیازمندی‌های دسترس‌پذیری در پروژه IoT-A شامل موارد زیر است. با مراجعه به این کدها در نیازمندی‌های دسترس‌پذیری پروژه IoT-A، می‌توان جزئیات آن‌ها را مشاهده کرد.<br>UNI.040, UNI.050, UNI.058, UNI.060, UNI.064, UNI.065, UNI.092, UNI.230, UNI.232, UNI.233, UNI.601, UNI.604, UNI.610, UNI.616, UNI.718 |

[۳۴۱] Implicit

[۳۴۲] Non-repudiation

[۳۴۳] Accountability

[۳۴۴] Failure

| | |
|---|---|
| کارایی | مرتبط با هر سیستمی که نیازمندی‌های دسترس‌پذیری گسترده یا پیچیده، فرآیندهای بازیابی پیچیده، یا یک پروفایل بزرگ (مثلا قابل مشاهده توسط عموم) دارد. |
| فعالیت‌ها | ۱- استخراج نیازمندی‌های دسترس‌پذیری<br>۲- ایجاد زمان‌بندی دسترس‌پذیری<br>۳- تخمین دسترس‌پذیری پلتفرم<br>۴- تخمین دسترس‌پذیری کاربردها<br>۵- ارزیابی نیازمندی‌ها<br>۶- دوباره کار انداختن[۳۴۵] معماری |
| راهبردها | ۱- انتخاب سخت‌افزاری که قابلیت تحمل خطا را داشته باشد<br>۲- استفاده از خوشه‌بندی بسیار دسترس‌پذیر و تعادل بار<br>۳- ثبت تراکنش‌ها<br>۴- استفاده از راه‌حل‌های دسترس‌پذیری نرم‌افزاری<br>۵- انتخاب یا ایجاد یک نرم‌افزار با قابلیت تحمل خرابی<br>۶- طراحی برای خرابی<br>۷- اجازه به هر جزء برای تکثیر<br>۸- رهاکردن سازگاری تراکنشی<br>۹- شناسایی راه‌حل‌های Backup و بازیابی هنگام حادثه |

## ۷-۲- معماری MGC[۳۴۶]

معماری MGC، یک معماری پیشنهادی برای IoT بر اساس رایانش ابری است که قرار است از پروژه SITP استخراج شود. در واقع، حجم بسیار بالای اطلاعات به دست آمده از طریق دستگاه‌های IoT باید به گونه‌ای پردازش شوند و واضح است که این پردازش، به پردازنده‌های بسیار قدرتمند احتیاج دارد که از طریق ابر میسر است. لذا معماری MGC پیشنهاد شد تا بتوان به نیاز پردازشی IoT پاسخ داد. این معماری شامل چهار بخش زیر است:

[۳۴۵] Rework

[۳۴۶] eMbedded devices Gateways Cloud

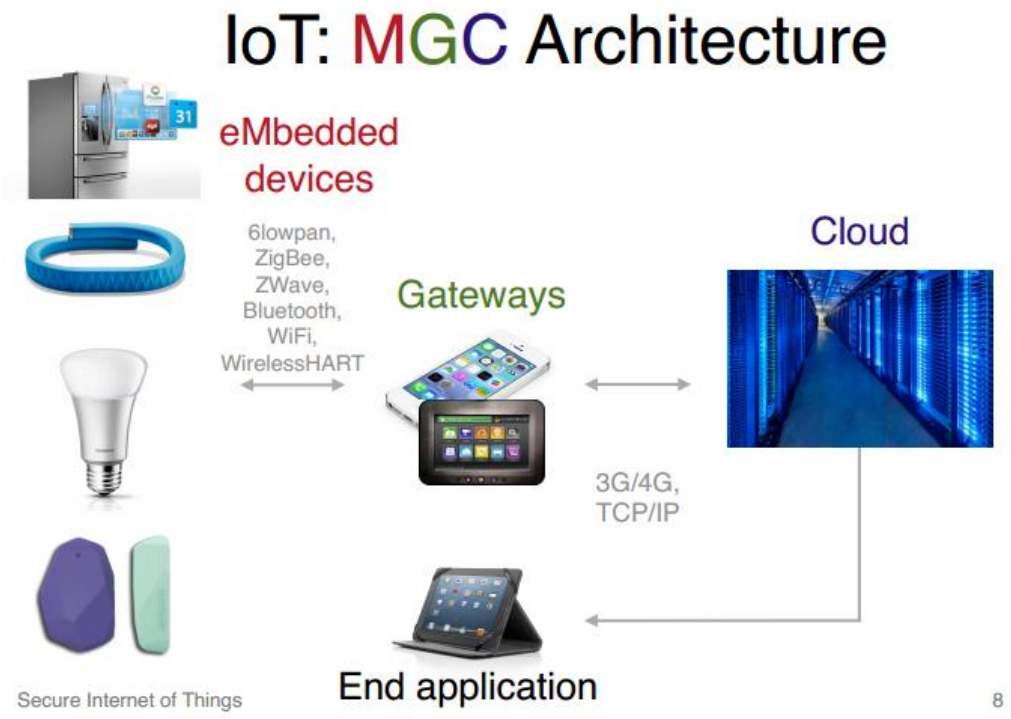
۱- دستگاه‌های فشرده: هر دستگاه با قابلیت اندازه‌گیری در این بخش قرار می‌گیرد. به عنوان مثال موبایل‌ها، حسگرها، محرک‌ها و تمام دستگاه‌های هوشمند در این بخش هستند.

۲- درگاه‌ها: سخت‌افزارهای واسط مورد نیاز برای ارتباط دستگاه‌ها با ابر، در زمره این بخش قرار می‌گیرند.

۳- ابر: پردازنده‌ای بسیار قوی است که اطلاعات جمع‌آوری شده را پردازش می‌کند و نتیجه را به کاربرد نهایی می‌فرستد.

۴- کاربرد نهایی: کاربرد مورد انتظار از سوی کاربر که به وسیله آن سرویس‌ها به کاربران ارائه می‌شود و نیازهای آن‌ها برطرف می‌گردد.

این چهار بخش توسط فناوری‌های مختلف به یکدیگر متصل می‌شوند. به عنوان مثال برای اتصال دستگاه‌ها به درگاه‌ها، از فناوری‌هایی مثل 6lowpan، ZigBee، ZWave، Bluetooth، WiFi و WirelessHART؛ و برای اتصال درگاه‌ها به ابر نیز از فناوری‌هایی مثل 3G/4G و TCP/IP استفاده می‌شود. شکل ۷-۲-۱-۱ این بخش‌ها و نحوه برقراری ارتباطات میان آن‌ها را نمایش می‌دهد.



شکل ۷-۲-۱-۱ معماری MGC

دستگاه‌های فشرده از پردازنده‌هایی مثل ARM، AVR و msp430 استفاده می‌کنند. همچنین ابر نیز برای برقراری ارتباط با درگاه‌ها و پردازش‌های خود از نرم‌افزارهایی مثل Ruby/Rails، Python/Django، J2EE، PHP و Node.js استفاده می‌نماید. علاوه بر این، کاربرد نهایی نیز از زبان‌های برنامه‌نویسی مثل Obj-C/C++، Java، Swift، Javascript/HTML استفاده می‌نماید.

## ۷-۲-۲- امنیت در معماری MGC

برای ایجاد امنیت در معماری MGC دو هدف عمده دنبال می‌شود:

۱- امنیت داده: بررسی و تعریف مدل‌های محاسباتی رمزنگاری جدید برای تحلیل‌های داده امن و به کار گرفتن آن‌ها در دنباله‌های داده متعدد و آنی در سیستم‌های فشرده

۲- امنیت سیستم: بررسی و اجرایی کردن یک چارچوب نرم‌افزاری/سخت‌افزاری امن کد باز[۳۴۷] که ساختن کاربردهای اینترنت اشیاء را با استفاده از مدل‌های محاسباتی جدید، ساده نماید.

### ۷-۲-۲-۱-امنیت داده

امنیت، آنچه که ما یک مهاجم می‌تواند انجام دهد را محدود می‌کند. اما نیازهای کاربردهای IoT اغلب شامل موارد زیر است:

- تولید نمونه‌های داده
- پردازش/فیلتر کردن این نمونه‌ها
- تحلیل دنباله‌های داده، با ترکیب تاریخچه آن‌ها
- ارائه نتایج برای کاربردها

اما در نهایت، برای امنیت، مهمترین هدف، امنیت پایان به پایان است. به این منظور نیز باید این موارد انجام شوند:

- دستگاه‌ها داده‌های رمز شده تولید نمایند

[۳۴۷] Open Source

- تنها کاربردهای پایانی بتوانند به طور کامل رمزگشائی را انجام دهند و داده‌ها را مشاهده کنند
- درگاه‌ها و ابر باید بتوانند روی داده‌ها عملیات انجام دهند، بدون اینکه از ماهیت اطلاعات با خبر باشند.

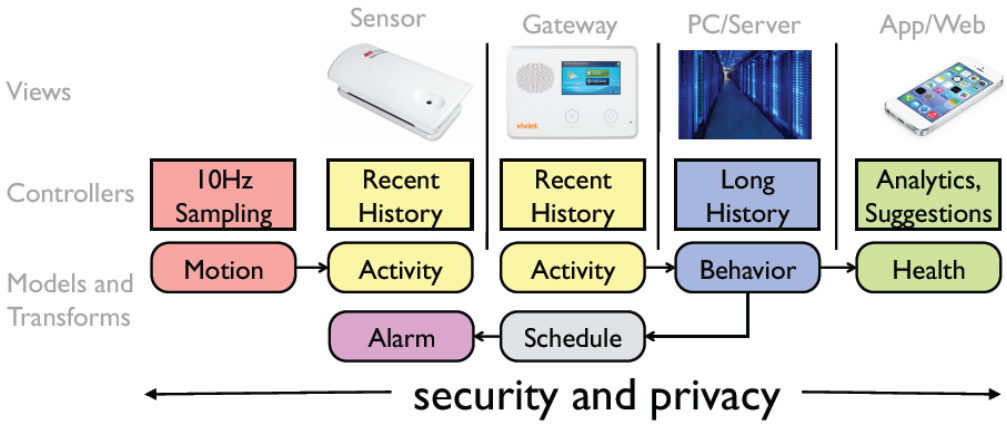
در پروژه SITP این نیازها به معرفی یک طرح مناسب و کارا برای رمزنگاری هومومورفیک ختم شده است و از جمله هدف‌های مهم این پروژه، پیشنهاد یک روش رمزنگاری هومومورفیک هست تا بتواند امنیت پایان به پایان را تضمین نماید. همچنین برای امن کردن آمارهای موجود باید مدل‌های محاسباتی رمزنگاری جدیدی پیشنهاد شود تا محاسباتی را که کاربردهای IoT نیاز دارند، پشتیبانی نماید. به عنوان مثال، یک راهکار، انجام پروتکل‌ها به صورت توزیع شده است که در این حالت، ابر نتایج را بدست می‌آورد، اما از داده‌هایی که آن نتایج را می‌دهند بی‌اطلاع است. همچنین به دلیل آنکه عمدتا در IoT، محاسبات امنیتی برای محیط‌های محدود و کم‌توان انجام می‌شود، سربار کم مخابراتی، تناوب دسترسی به شبکه و سایر شرایط محدود کننده نیز باید در طراحی در نظر گرفته شوند.

### ۷-۲-۲-۲- امنیت سیستم

انجام پردازش داده‌ها به مراحل زیر احتیاج دارد که در همه آن‌ها باید امنیت و حریم خصوصی در نظر گرفته شود:

- مجموعه مدل‌ها که در هنگام ذخیره داده‌ها، آن‌ها را توصیف می‌کنند
- انتقال داده‌ها بین مدل‌ها
- نمونه‌های مدل‌ها به دستگاه‌ها محدود هستند
- مشاهدات می‌توانند مدل‌ها را نمایش دهند
- کنترل کننده‌ها مشخص می‌کنند که چگونه داده‌ها انتقال یابند

شکل ۷-۲-۲-۱ مشخص کننده مراحل پردازش داده است و مراحل فوق به صورت دقیق در آن قابل مشاهده است:




شکل ۷-۲-۲-۱ مراحل پردازش

در ادامه، چارچوب سیستم، یک ساختار کد برای کل این مراحل ایجاد می‌کند که طراح می‌تواند این کد ایجاد شده را برای تحقق نیازمندی‌های خود اصلاح نماید. در این حین، چارچوب مشخص شده به طور مداوم بررسی می‌کند که اصلاحیه‌های انجام شده توسط طراح، از معماری مطرح شده برای پردازش تخطی نکند. علاوه بر این، نوع داده‌ها، نشت اطلاعات و رمزنگاری نیز بررسی می‌شوند. ضمن این مسأله، چاچوب مطرح شده، باید به طور اتوماتیک مسأله پروتکل‌های بسیار کم‌توان، پیچیدگی‌های لایه ارتباطی و عدم تطبیق پروتکل‌ها را نیز توسط الگوریتم‌های شبکه جدید حل کند. رویکرد پیاده‌سازی امنیت و حریم خصوصی نیز به سمت استفاده از سخت‌افزارهای تعریف شده توسط نرم‌افزار[۳۴۸] است، ضمن اینکه سادگی نیز باید در تمامی موارد رعایت شود.

## ۷-۳- معماری‌های SOA[۳۴۹] و Compose[۳۵۰]

معماری‌های SOA و Compose هر دو برای کاربرد در اینترنت اشیاء پیشنهاد شده‌اند و از نظر ساختاری بسیار مشابه هستند. به طور کلی این دو معماری از پنج لایه اشیاء، چکیده اشیاء (سرویس اشیاء)، مدیریت سرویس

[۳۴۸] Software-defined Hardware

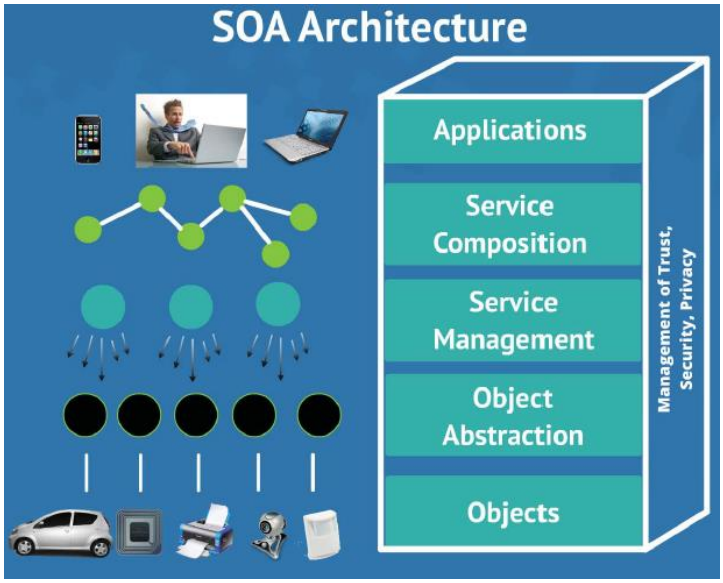
[۳۴۹] Service Oriented Architecture

[۳۵۰] Collaborative Open Market to Place Objects at your Service

(سرویس‌ها)، ترکیب سرویس (فروشگاه سرویس‌ها) و کاربرد (ذی‌النفعان) تشکیل شده‌اند. در معماری Compose به سه لایه میانی اصطلاحا بازار باز[۳۵۱] گفته می‌شود. در ادامه به معرفی مختصر این دو معماری می‌پردازیم.

### ۷-۳-۱- معماری SOA

شکل ۷-۳-۱-۱، شمای کلی معماری SOA را نشان می‌دهد.



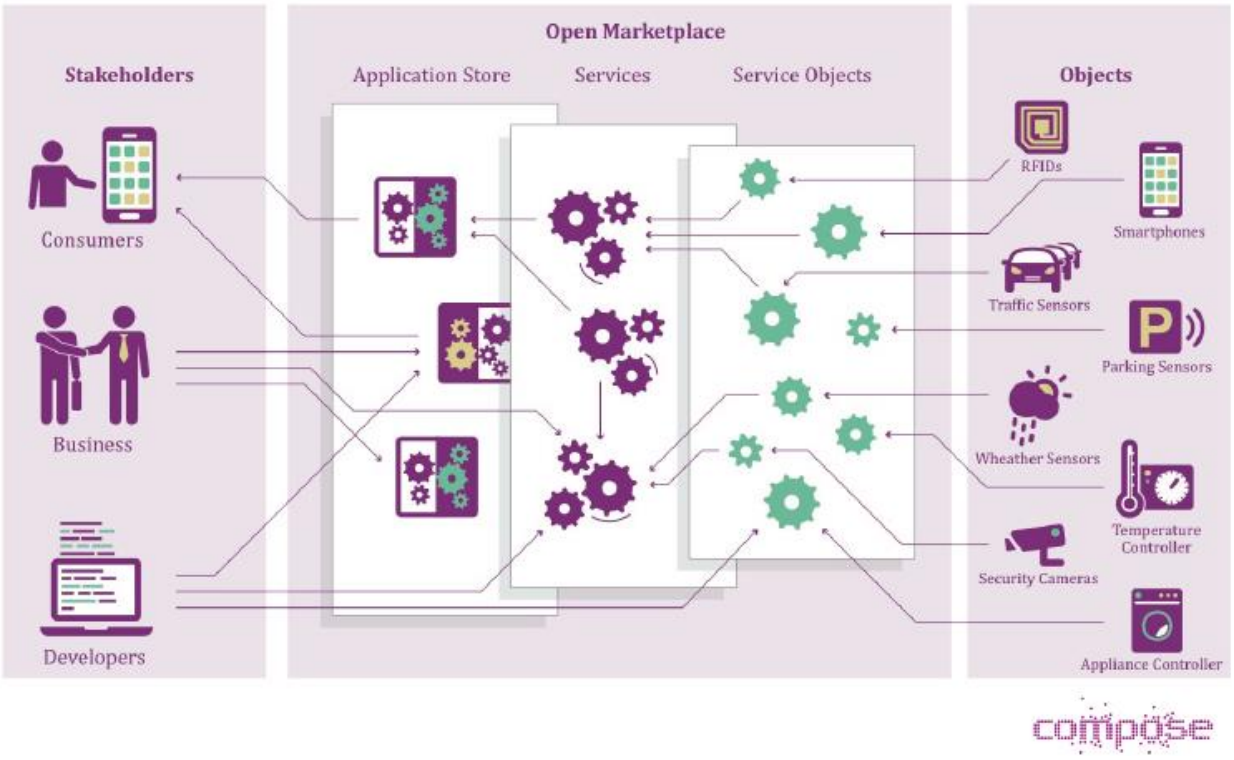

شکل ۷-۳-۱-۱معماری SOA

از آنجا که تشابه معماری Compose با SOA بسیار زیاد است، به توضیح معماری Compose بسنده شده است.

### ۷-۳-۲- معماری Compose

شکل ۷-۳-۲-۱، شمای کلی معماری Compose را نشان می‌دهد. هزینه پروژه Compose 7.4M€ است که 5.3M€ از آن توسط اتحادیه اروپا تأمین می‌شود.

[۳۵۱] Open Marketplace




**شکل ۷-۳-۲-۱ معماری Compose**

معماری Compose به طور کلی شامل موارد زیر است:

- یک اکوسیستم متناسب با IoT ارائه می‌دهد
- به راحتی و به صورت امن، سرویس‌ها را بر اساس اشیاء هوشمند متصل به اینترنت، ایجاد می‌کند، گسترش می‌دهد، به اشتراک می‌گذارد و نگهداری می‌کند.
- استخراج شده از موقعیت‌های استفاده
- تمام چرخه عمر سرویس را می‌پوشاند
- زنجیره‌های ارزش و مدل‌های تجاری جدید را شناسایی و بررسی می‌کند
- پذیرش و استانداردسازی را ارتقاء می‌دهد.

رویکرد فنی معماری Compose نیز یک بازار اشیاء سرویس‌ها برای ارائه موارد زیر است:

- مدیریت سرویس اشیاء
  - ثبت، مجازی‌سازی تراکنش و شیء، نگهداری، حسابرسی، تراکم و ارسال آگاهی
- طراحی سرویس و محیط اجرا

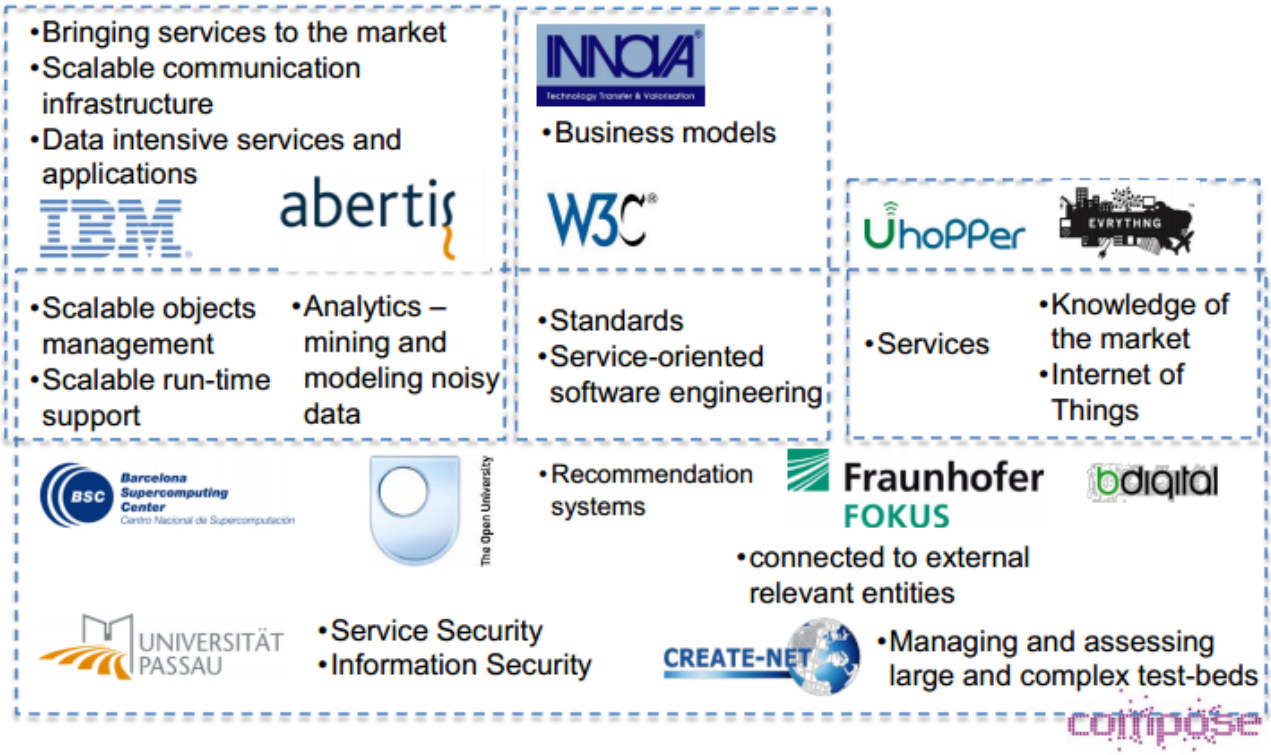
- SDK برای توسعه و گسترش آسان سرویس‌ها بر اساس اشیاء متصل شده به اینترنت
- محیط زمان اجرا (برای هر دوی سرورها و دستگاه‌های موبایل) به منظور پیکربندی پویا و اجرایی کردن سرویس‌ها

- ارائه یک لایه میان‌افزار متناسب با IoT
  - ساختن روی فناوری موجود برای ایجاد یک اکوسیستم پایان به پایان برای IoT
  - عملکردهای سیستم توزیع شده
  - تجمیع بی‌درز گروهی از اشیاء به وسیله چکیده کردن آن‌ها در اشیاء سرویس به طوری که ردیابی‌پذیری و وابستگی را تضمین نمایند.

همچنین پیشران‌های Compose نیز سه حوزه زیر می‌باشد:

- تجربیات فروشگاهی (فضای هوشمند)
- شهر هوشمند (بارسلونا)
- استان هوشمند

کنسرسیوم Compose نیز مطابق شکل ۷-۳-۲-۲ است.




شکل ۷-۳-۲-۲ کنسرسیوم Compose

## ۷-۴- معماری WOA[۳۵۲]

http://en.wikipedia.org/wiki/Web-oriented_architecture

http://www.gartner.com/it-glossary/web-oriented-architecture-woa

تعریف رسمی Gartner از معماری WOA این چنین است:

معماری WOA، یک نسخه بهبود یافته از معماری SOA است که کاربران و سیستم‌ها را با یک وب ابررسانه جهانی[۳۵۳] بر اساس معماری وب تجمیع می‌کند. این معماری روی عمومیت رابط[۳۵۴]ها (رابط‌های کاربری و APIها) تأکید دارد تا به اثرات جهانی شبکه در پنج قید اساسی رابط‌ها دست یابد:

---

[۳۵۲] Web-Oriented Architecture

[۳۵۳] Web of globally linked hypermedia

[۳۵۴] Interface

- شناسایی منابع
- دستکاری منابع در نمایش
- پیام‌های خود توصیف
- ابررسانه به عنوان موتور حالت کاربرد
- بی‌طرفی کاربرد

به نوعی می‌توان ویژگی‌های WOA را حاصل جمع ویژگی‌های SOA، WWW و REST[۳۵۵] در نظر گرفت.

در واقع WOA، یک مجموعه از پروتکل‌های وب مثل HTTP و XML است که تنها تفاوت آن با SOA، قرار گرفتن REST در آن است (REST یک روش ساده، قدرتمند و محبوب به کارگیری پروتکل HTTP به عنوان سرویس وب است).

### ۷-۴-۱- مقایسه WOA و SOA

مهمترین تفاوت میان SOA و WOA آن است که WOA از REST پشتیبانی می‌کند، حال آنکه SOA از SOAP استفاده می‌کند.

- SOAP از XML استفاده می‌کند که یک فرمت پیام، شامل تمام اطلاعات سرآیند و امنیت است و اطلاعات را به وسیله یک ساختار ویژه منتقل می‌کند، اما REST این مشکل را با انتقال اطلاعات به شکل URL، حذف می‌نماید.
- SOA از WS-Security استفاده می‌کند، حال آنکه WOA از HTTPS، OAuth و HMAC-SHA-1 بهره می‌برد.
- REST به سیستم‌ها اجازه می‌دهد تا با استفاده از URLها، به صورت کارا به عملیات با یکدیگر بپردازند.

OAuth یکی از بالاترین معیارهای امنیتی در اینترنت امروزی است که توسط تعداد زیادی از وبسایت‌ها مثل Twitter مورد استفاده قرار می‌گیرد. موضوعات شناسایی می‌تواند یک مسأله مهم برای کاربردهای WOA باشد و

[۳۵۵] Representational state transfer

روش WOA در بسیاری از کاربردهای ابری مورد استفاده قرار می‌گیرد. همچنین، بیشتر طراحی‌های WOA شامل یک لاگین فدرال هستند که امکان تأیید هویت کاربرد را ساده‌تر می‌کند و برای کاربر نیز برای حرکت بین برنامه‌ها ساده‌تر است.

پشته WOA نیز شامل موارد زیر است:

- توزیع (HTTP، feeds)
- ترکیب (Hypermedia، Mashups)
- امنیت (OpenID، SSL)
- انتقال‌پذیری داده (XML، RDF)
- ارائه داده (ATOM، JSON)
- روش‌های انتقال (REST، HTTP، BitTorrent)

## ۷-۵- سایر معماری‌های دیگر

در این بخش برخی معماری‌های پیشنهادی دیگر برای اینترنت اشیاء معرفی می‌گردند.

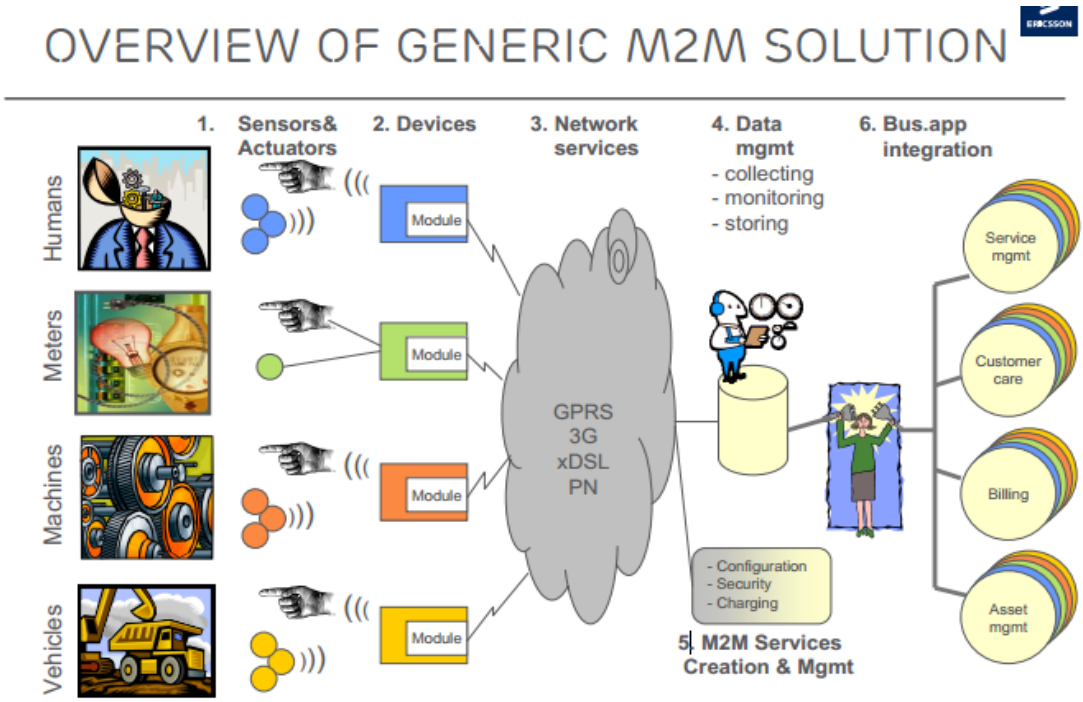
### ۷-۵-۱- معماری پیشنهادی شرکت اریکسون

[Haghighi Report]

معماری مفهومی ارائه شده توسط شرکت اریکسون در حقیقت همان معماری سرویس‌گرا است. با این حال لایه‌هایی که آنها برای معماری اینترنت اشیاء تعریف نموده‌اند با لایه‌هایی که سایر معماری‌ها پیشنهاد داده‌اند اندکی متفاوت است. در پایین‌ترین لایه، شرکت اریکسون اشیاء را قرار داده است.

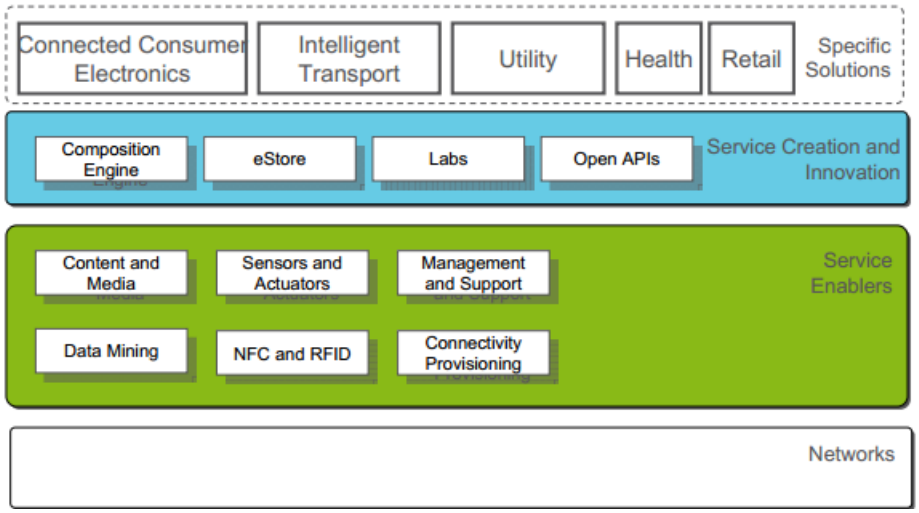
معماری پیشنهادی اریکسون برای اینترنت اشیاء (در حقیقت اینترنت متصل کننده ماشین به ماشین یا M2M) در شکل ۷-۵-۱-۱ نمایش داده شده است. توجه کنید که لایه Data Management و لایه M2M Services Creation & Management در حقیقت نقطه تفاوت اصلی معماری اینترنت فعلی و معماری سرویس گرای اینترنت اشیاء هستند. این دو لایه هستند که حسب درخواست کاربر (یا برنامه کاربردی)، اشیاء و اطلاعات لازم برای به انجام

رساندن وظیفه را به خدمت فرا می‌خوانند. شبکه در این معماری، تنها یک کانال ارتباطی است و تنها یک لایه از اینترنت آینده را تشکیل می‌دهد.




شکل ۷-۵-۱-۱ معماری پیشنهادی اریکسون برای اینترنت اشیاء

از منظر خدمات رسانی (Service Delivery) معماری دیگری توسط اریکسون پیشنهاد شده است. این معماری با معماری کلی شکل قبل در تضاد نیست، بلکه از دیدگاه دیگری مسأله را نشان می‌دهد. به طور دقیق‌تر، این معماری بر اساس معماری کلان قبلی کار می‌کند. شکل ۷-۵-۱-۲ معماری خدمات رسانی پیشنهادی توسط اریکسون را نشان می‌دهد.




شکل ۷-۵-۱-۲معماری پیشنهادی اریکسون برای خدمات رسانی در اینترنت اشیاء

نکته جالب توجه آن است که نحوه خدمات رسانی از شکل کلاسیک اینترنت فاصله گرفته است. در شکل کلاسیک خدمات رسانی برنامه‌های کاربردی به صورت عمودی و بشکل سیلو وار روی منابع شبکه (اینترنت) پیاده سازی می‌شوند. این بدان معنی است که هر برنامه کابردی منابع خود را از شبکه برمی‌دارد و یا از آن به طور مستقل استفاده می‌کند و با این منابع یک خدمت را ارائه می‌دهد. در شکل معماری پیشنهادی اریکسون، معماری به حالت افقی درآمده است. به طور دقیق‌تر، برنامه‌ها روی یک بستر سوار می‌شوند که امکان به اشتراک گذاری منابع (اطلاعات، شبکه و اشیاء) را فراهم می‌کند. در شکل فوق این مسأله به وضوح دیده می‌شود. شبکه در لایه پایین تنها کانال ارتباطی را مهیا می‌کند (همان مفهوم معماری کلی). روی این کانال ارتباطی توانمندسازهای خدمات قرار می‌گیرند که در واقع اشیاء، سنسورها و غیره را می‌توان در این لایه دید. لایه بعدی لایه مدیریت و خلق سرویس است که بطور کلاسیک یک لایه معماری سرویس‌گرا است و برای ارضاء نیازمندی‌های برنامه کاربردی لایه بالا، منابع لایه پایین را بر حسب صلاحدید خود انتخاب و استفاده می‌کند. این معماری خدمات رسانی، امکان استفاده مشترک از اشیاء را فراهم می‌کند و برنامه‌های کاربردی را را از حالت سیلو وار و مستقل خارج می‌کند.

### ۷-۵-۱-۱-۲- سکوی ارتباط اشیاء (Device Connection Platform)

[T. H. Miguel Blockstrand, lars-Örjan kling, Robert Skog and Berndt Wallin Operator opportunities in the internet of things, Ericsson review, 2011.]

اریکسون با چشم‌انداز اتصال ۵۰ میلیارد شیء به یکدیگر، پیش‌بینی لزوم وجود یک سکو برای این ارتباطات را کرده و سعی نموده آن را طراحی کند. در مرجع این بخش، این سکو توصیف شده است. قبل از بیان مفاهیم و اشکال، مروری بر جدول اختصارات زیر خواهیم داشت (جدول ۷-۵-۱-۱). ذکر این نکته ضروری است که با توجه به تخلیص مواد مرجع فوق الذکر، تمامی این اختصارات در این گزارش استفاده نخواهند شد.

**جدول ۷-۵-۱-۱ اختصارات احتمالی مورد استفاده در توصیف سکو و معماری ارتباط اشیای اریکسون**

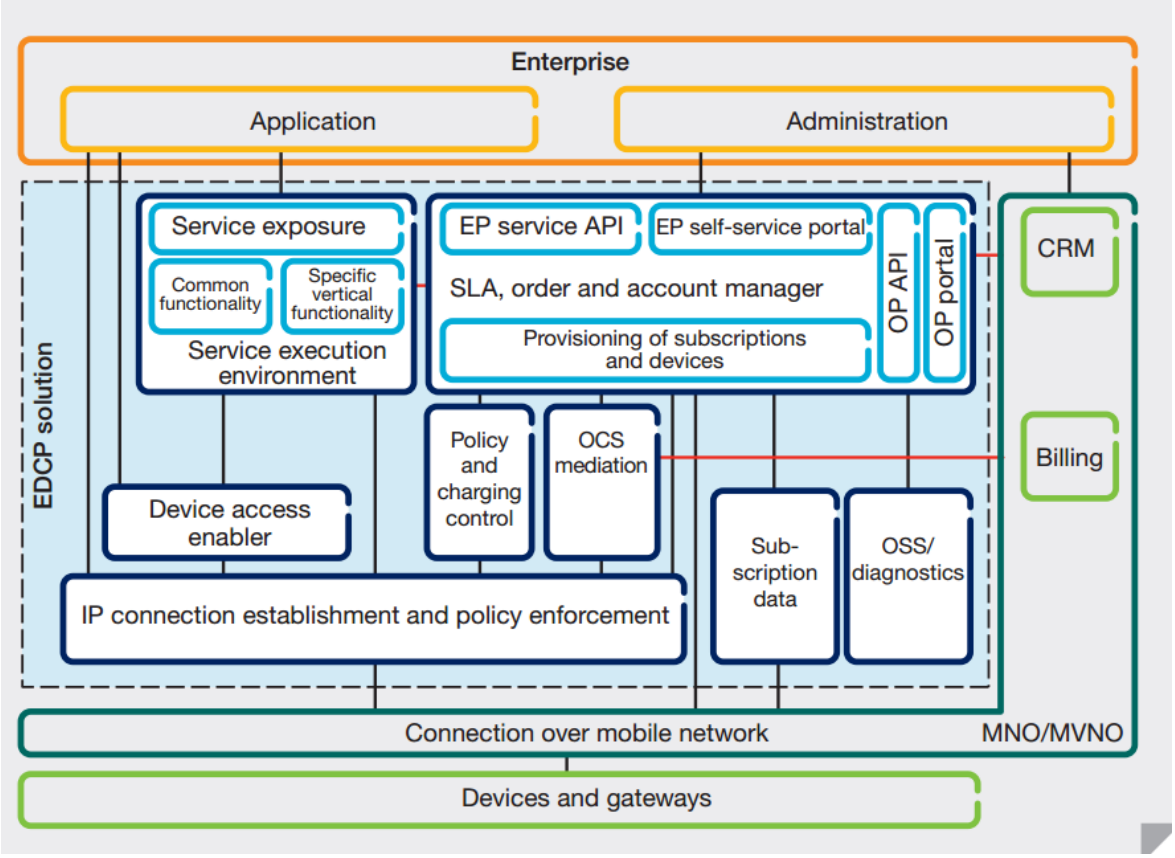
| | | | | | |
|---|---|---|---|---|---|
| 3GPP | 3rd Generation Partnership Project | GSM | Global System for Mobile Communications | OCS | online charging system |
| ACL | access control list | HLR | home location register | OSS | Operational Support System |
| API | Application Programming Interface | HTTP | Hypertext Transfer Protocol | PDC | Personal Digital Cellular |
| APN | Access Point Name | IETF | Internet Engineering Task Force | PDP | Packet Data Protocol |
| AUC | authentication center | IMSI | International Mobile Subscriber Identity | PLMN | Public Land Mobile Network |
| CDR | Call Detail Record | IP | Internet Protocol | QoS | quality of service |
| CoAP | Constrained Application Protocol | IPTV | IP TV | RADIUS | Remote Authentication Dial-In User Service |
| CRM | customer relationship management | IPv4 | IP version 4 | SaaS | software as a service |
| DAE | Device Access Enabler | IPv6 | IP version 6 | SGSN | Serving GPRS Support Node |
| DNS | Domain Name System | M2M | machine-to-machine | SIM | subscriber identity module |
| EDCP | Ericsson Device Connection Platform | MCC | Mobile Country Code | SLA | Service Level Agreement |
| GGSN | Gateway GPRS Support Node | MNC | Mobile Network Code | SMS | Short Message Service |
| Gn | IP based interface between the SGSN and other SGSNs and (internal) GGSNs | MNO | mobile network operator | SMS-C | Short Message Service Center |
| Gp | IP-based interface between the internal SGSN and external GGSNs | MSC | mobile switching center | SSL | Secure Sockets Layer |
| Gr | Interface between SGSNs and HLRs. Messages going through this interface use the MAP3 protocol | MSIN | Mobile Station Identification Number | VPN | virtual private network |
| | | MVNO | mobile virtual network operator | WAP | Wireless Application Protocol |
| | | NAT | Network Address Translation | WCDMA | Wideband Code Division Multiple Access |

همان‌طورکه دیده می‌شود، این سکو با نام اختصاری EDCP نشان داده می‌شود. شکل ۷-۵-۱-۲ راه‌حل سکوی پیشنهادی و نحوه ارتباط برقرار کردن آن با سازمان‌های بزرگ و اپراتورهای موبایل را نشان می‌دهد. این معماری کارکرد را در سه حوزه زیر تأمین می‌کند:

- ارتباط اشیاء
- سیاست کنترل و شارژ (کسر از حساب)
- مدیریت و تدارکات اشیاء و اشتراک[۳۵۶]

[۳۵۶] Subscriptions

اشیاء به برنامه‌های کاربردی سازمان‌های بزرگ از طریق شبکه موبایل اپراتور متصل می‌شوند.




**شکل ۷-۵-۱-۲ معماری درونی سکوی اریکسون برای ارتباط اشیاء (EDCP)**

DAE (Device Access Enabler) اجازه دسترسی به اشیاء را در بستر اینترنت کنترل و مدیریت می‌کند. بلوک کنترل شارژ و سیاست[۳۵۷]، تنظیمات خاص اشتراکات نظیر تعیین سقف مصرف داده و میزان شارژ (هزینه) را معین می‌کند. برای اپراتورها و کاربران سازمانی، پورتال اختصاصی برای دسترسی به سکو برای مدیریت سفارشات، حساب‌ها و نیز SLA[۳۵۸] فراهم می‌شود. به عنوان مثال، اپراتور می‌تواند اشتراک مخصوص enterprise را ایجاد، پورتال را تنظیم و گزارشات SLA را پایش کند. برای مثال از طریق پرتال، یک سازمان (enterprise) می‌تواند خدماتی را خریده، سیم کارت‌هایی را سفارش و داده‌های دستگاه‌ها و اشیاء را به صورت بلا درنگ و یا به شکل کلان و آماری مشاهده کند.

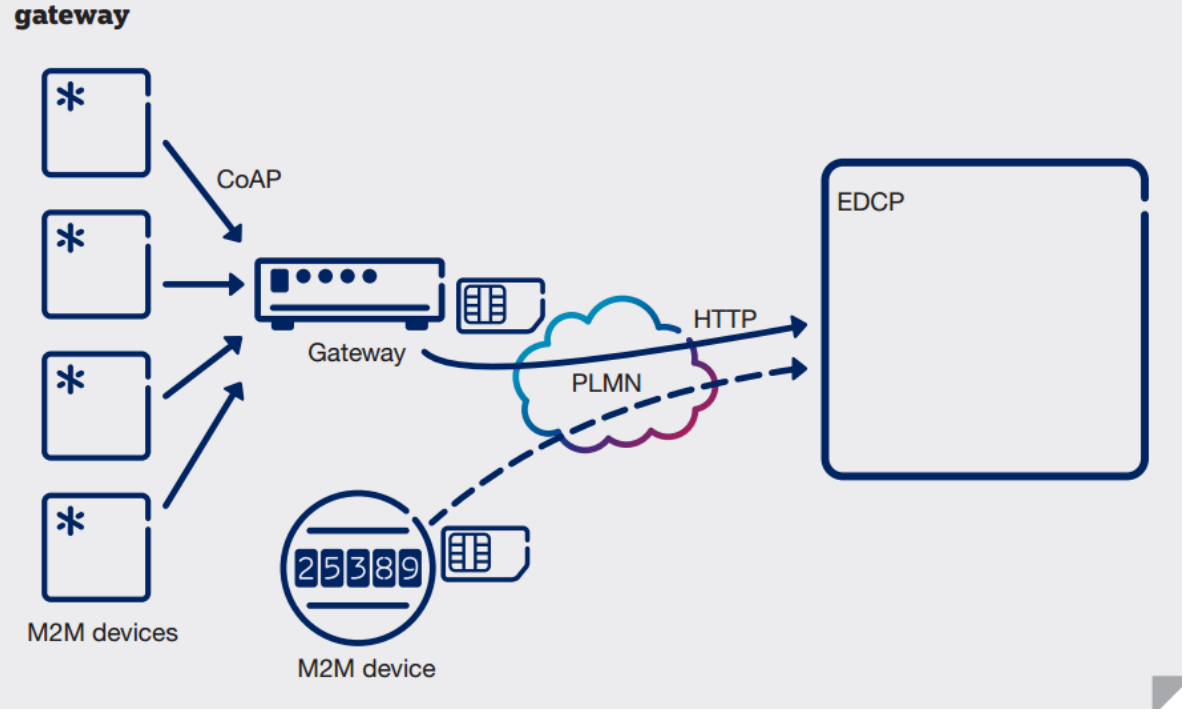
[۳۵۷] Policy and Charging Control

[۳۵۸] Service Level Agreement

همه اشیاء توسط EDPC حمایت و در پایگاه داده عضو می‌شوند. باکس OSS/Diagnostics کارکردهای عملیاتی و نگهداری و مراقبتی مانند مدیریت هشدار و نیز آماردهی برای گزارش SLA را تهیه و تدارک می‌بینند. بخشی از این اطلاعات وضعیت و هشدارها برای مرکز کنترل عملیات شبکهٔ[۳۵۹] اپراتور ارسال شده و در آنجا مورد استفاده قرار می‌گیرد.

البته همه اشیاء نمی‌توانند از طریق سیم کارت به یکدیگر متصل شوند. شکل زیر سناریو دیگری را بیان می‌نماید که محتمل‌تر است. در این سناریو اشیاء از طریق یک درگاه (درگاه) به EDCP متصل می‌شوند.

همان‌طور که در شکل ۷-۵-۱-۳ می‌بینیم، اشیاء از طریق یک درگاه به عنوان مثال موبایل فرد به شبکه اینترنت متصل می‌شوند، اما همگی به صورت M2M[۳۶۰] با هم مرتبط هستند. EDCP به عنوان یک SaaS[۳۶۱] پیاده‌سازی می‌شود و به این ترتیب از تسهیلات شارژ، ارتباط و غیره پشتیبانی نموده و با نودهای مختلف ارتباط برقرار می‌کند.




[۳۵۹] Network Operation Center (NOC)

[۳۶۰] Machine to Machine

[۳۶۱] Software as a Service

شکل ۷-۵-۱-۳ ارتباط سکوی EDCP اریکسون با اشیاء از طریق یک درگاه

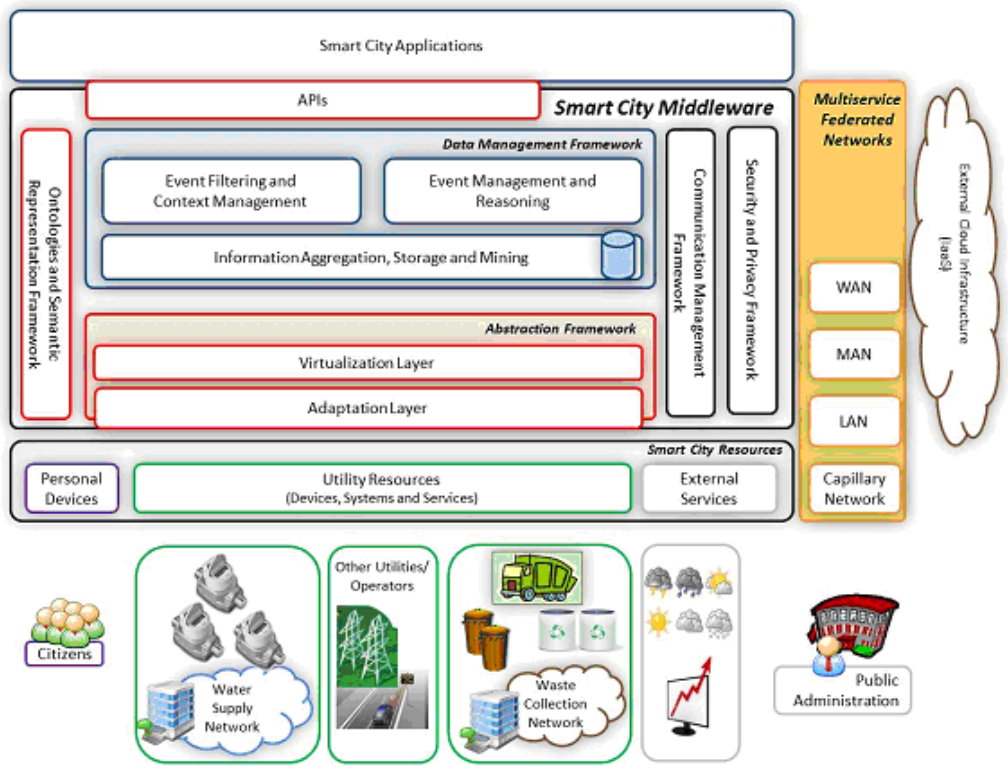
## ۷-۵-۲- معماری پیشنهادی اینترنت اشیاء برای شهر هوشمند – پروژه ALMANAC

[Haghighi Report]

ALMANAC نام پروژه‌ای است که بخش اعظم آن توسط اتحادیه اروپا و ذیل برنامه هفتم توسعه اتحادیه اروپا برای تحقیق و توسعه در زمینه اینترنت اشیاء برای شهری هوشمند[۳۶۲] حمایت مالی می‌شود. منطق این شهر بر اساس فناوری اینترنت اشیاء است. در این شهر کلیه اشیاء فیزیکی دارای یک جنبه مجازی نیز هستند و این اشیاء با یکدیگر ارتباط برقرار نموده و تصمیم گیری می‌کنند.

سکوی ALMANAC، اطلاعات را به صورت هم‌زمان و یا تقریبا هم‌زمان از حسگرها و عملگرهای مختلف در سرتاسر شهر گردآوری کرده و آنها را تجمیع و تحلیل می‌کند تا در فرآیندهای لازم برای هوشمندسازی یک شهر هوشمند مورد استفاده قرار گیرند. هسته اصلی این سکو یک معماری SOA دارد و تعامل بین اشیاء، خدمات و نیز مدیریت داده و منابع را ممکن می‌کند. شکل ۷-۵-۲-۱ معماری سکوی ارتباطی ALMANAC برای شهر هوشمند را نشان می‌دهد.

[۳۶۲] Smart City




**شکل ۷-۵-۲-۱معماری پیشنهادی برای سکوی شهر هوشمند ALMANAC**

همان‌طور که ملاحظه می‌شود، این معماری بسیار شبیه معماری‌های سرویس‌گرای قبلی است. به همین دلیل از ذکر جزئیات خودداری می‌کنیم. توجه کنید که این معماری مربوط به شهر هوشمند است. معماری مرجع مورد استفاده برای ارتباطات ماشین با ماشین و یا شیء با شیء (M2M) که به صورت میان‌افزار در این معماری و در مغز آن استفاده می‌شود، یک معماری SOA، مانند آنچه در IoT-A شرح داده شد، است. در این معماری‌ها پشته IoT شامل سه لایه اشیاء، درگاه‌ها، و هسته مرکزی IoT است که در هر لایه موارد زیر قابل به کارگیری است:

- مدیریت داده‌های اینترنت اشیاء[۳۶۳]: ذخیره محلی، بافرها، تجمیع داده، کنترل خطا
- ارتباطات اینترنت اشیاء[۳۶۴]: تبدیل بین پروتکل‌های لایه بالا و پایین
- مدیریت منابع اینترنت اشیاء[۳۶۵]: مجازی‌سازی سنسورها، اشیاء و غیره

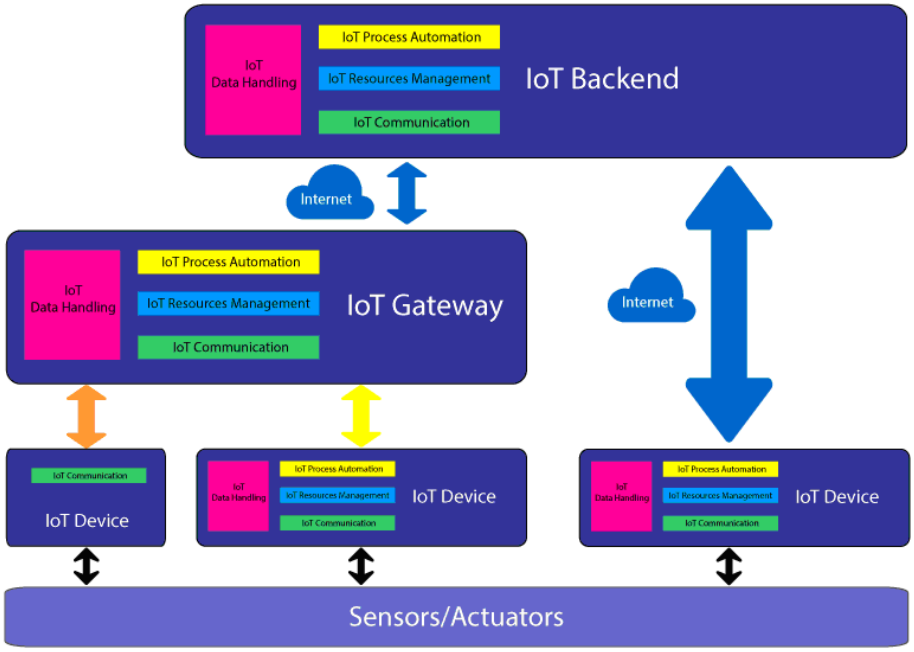
[۳۶۳] IoT Data Handling

[۳۶۴] IoT Communication

[۳۶۵] IoT Resource Management

- خودکارسازی فرآیند اینترنت اشیاء[۳۶۶]: اجرای دستورات و قواعد محلی، مدیریت فراداده[۳۶۷]

شکل کلاسیک معماری مرجع اینترنت اشیاء در شکل ۷-۵-۲-۲ نشان داده شده است. همان‌گونه که ملاحظه می‌شود، اشتراکات مفهومی زیادی میان این معماری و معماری پیشنهادی اریکسون نیز دیده می‌شود. در هر دو مورد اینترنت کنونی (شبکه)، تنها کانال ارتباطی است و اشیاء را به هم متصل می‌کند. اشیاء همانند مدل پیشنهادی اریکسون یا به طور مستقیم و یا با واسطی به نام درگاه به هسته اصلی شبکه اینترنت اشیاء متصل می‌شوند.




**شکل ۷-۵-۲-۲ معماری مرجع اینترنت اشیاء (مورد استفاده در ALMANAC)**

## ۷-۶- تجمیع معماری‌های پیشنهادی برای اینترنت اشیاء

[Haghighi Report]

[۳۶۶] IoT Process Automation

[۳۶۷] Meta data Management

همان‌گونه که در این بخش دیده شد، اکثر معماری‌های پیشنهادی برای اینترنت اشیاء از SOA الهام گرفته‌اند و با اندکی تغییر، همگی دارای لایه‌های مشابهی می‌باشند. به طور خلاصه، در لایه پایین اشیاء قرار داشته و روی آنها یک لایه که وظیفه تهیه خلاصه از کارکردها و وضعیت شیء را دارد، قرار می‌گیرد. برنامه‌های کاربردی و کاربران در بالاترین لایه قرار دارند. یک برنامه کاربردی به چند منبع و عنصر برای انجام وظیفه‌اش نیاز دارد. شکست نیازمندی در یک لایه زیرین آن رخ می‌دهد و سپس لایه‌ای دیگر آن نیازمندی‌ها و منابع را در میان انبوهی از خلاصه‌های تهیه شده از اشیاء و اطلاعات جستجو و پیدا می‌کند.

برای ایجاد امنیت در معماری‌های مطرح شده، معمولا یک درگاه یا فایروال در میان همه ارتباطات وجود دارد که مدیریت امنیت بر عهده آن است. عملی‌ترین روش امن‌سازی نیز استفاده از درگاه‌ها برای اتصال اشیاء به شبکه است.

هم اکنون نسخه‌های توسعه یافته‌تر SOA مثل WOA ارائه شده است که همان‌طور که بحث شد، علاوه بر ویژگی‌های SOA، دارای قابلیت‌های تکمیل کننده دیگری نیز هست و می‌توان این نسخه‌ها را به عنوان پایه معماری و معماری امنیتی برای اینترنت اشیاء در نظر گرفت. همچنین توصیه‌های صادر شده از طرف IoT-A نیز می‌تواند مسیر روشنی را برای امن‌سازی معماری‌های SOA و WOA نشان دهد.

## ۸- جمع‌بندی و نتیجه‌گیری

گزارش حاضر، یک بررسی جامع روی اینترنت اشیاء به همراه نیازمندی‌های امنیتی، حریم خصوصی و اعتماد آن ارائه داد. به این منظور ابتدا با تعریف اینترنت اشیاء و حوزه‌های تحقیق و توسعه، خواننده را برای ورود به بحث آماده کردیم. همچنین با دسته‌بندی اینترنت اشیاء از دیدگاه‌های مختلف، سعی کردیم تا جامعیت این مفهوم را روشن سازیم. بعد از این موارد، چشم‌انداز، اهمیت و اهداف اینترنت اشیاء بیان شد و سپس، پیشران‌های اقتصادی، امنیتی (کنترل دسترسی و مجوز استفاده) و تجاری آن مطرح شد. همچنین مزیت‌ها، کاربردها و حوزه‌های متأثر از IoT نیز بیان شد. سپس برخی مراکز معتبر پژوشی در زمینه اینترنت اشیاء بررسی شدند که در بین آن‌ها، مؤسسات و مراکز تحقیقاتی معتبر، شرکت‌های سهامی و شرکت‌های دانش‌بنیان، دانشگاه‌ها و آزمایشگاه‌های مهم قرار دارد. در فصل ۴، پروژه‌های تحقیقاتی امنیت و حریم خصوصی مرتبط با اینترنت اشیاء در ۱۰ شرکت برتر از دیدگاه مؤسسه گارتنر مورد بررسی قرار گرفتند و توضیحاتی اجمالی برای آن‌ها ارائه گردید. علاوه بر این، پروژه‌های تحقیقاتی امنیت و حریم خصوصی IoT در برنامه هفتم توسعه اتحادیه اروپا و همینطور برخی پروژه‌های مهم دیگر نیز بررسی شدند. با بررسی این پروژه، نیازمندی‌های امنیتی، حریم خصوصی و اعتماد اینترنت اشیاء استخراج گردید که مطالب مربوط به آن در فصل ۵ جای گرفتند. در فصل ۶ نیز چالش‌های کلی و مشکلات امنیتی اینترنت اشیاء مورد بررسی قرار گرفت و راه‌حل‌ها و رویه‌های پیشنهادی برای پاسخ به آن‌ها مطرح شد. این چالش‌ها به دو دسته مسائل مربوط به جمع‌آوری اطلاعات و مسائل مربوط به ارتباطات در اینترنت اشیاء تقسیم‌بندی شد که امنیت در همه آن‌ها دخیل می‌باشد. همچنین چالش‌های امنیتی، از دیدگاه حریم خصوصی و اعتماد نیز مورد بررسی قرار گرفتند و راه‌حل‌های ممکن پیشنهاد شد. در فصل ۷ نیز برخی معماری‌های مطرح شده برای IoT و امنیت در آن‌ها بیان گردید که مهمترین آن‌ها، معماری ARM (خروجی پروژه IoT-A در برنامه هفتم توسعه اتحادیه اروپا) است. از دیگر معماری‌های بررسی شده، SOA، Compose و WOA بود که اطلاعات آن‌ها در بخش‌های مرتبط موجود است.

در بررسی‌های صورت گرفته، مهمترین مسأله، عدم وجود یک معماری امنیتی تأیید شده برای IoT است. با توجه به نیازمندی‌های امنیتی (امنیت، حریم خصوصی و اعتماد) استخراج شده و معماری‌های پیشنهادی فوق، به نظر می‌رسد که ترکیب معماری‌های IoT-A و WOA بتواند یک معماری بسیار مناسب برای پوشش مسائل امنیتی مرتبط

با اینترنت اشیاء باشد. در واقع، IoT-A توصیه‌های لازم جهت یکپارچه‌سازی و سازگاری معماری امنیتی با تمام دستگاه‌ها را ارائه می‌دهد و WOA نیز روند دقیق استفاده از فناوری IoT را در عمل مشخص می‌کند که تحت توصیه‌های امنیتی IoT-A باید عمل کند.

در فاز دوم این پروژه، ابتدا امنیت معماری‌ها به طور کلی بررسی خواهد شد. سپس اهداف و راهبردهای پژوهشی برخی مؤسسات دیگر در زمینه امنیت اینترنت اشیاء بیان می‌شود. در ادامه پروژه‌های امنیتی مطرح شده در فاز اول به طور مفصل شرح داده و اولویت‌بندی می‌شوند. در نهایت نیز یک طرح و برنامه جامع برای پژوهشی در زمینه اینترنت اشیاء در ایران پیشنهاد می‌شود و پروژه‌های لازم نیز معرفی می‌گردند.

# ۹- واژه‌نامه و مراجع

در این فصل، واژه‌نامه و مراجع ارائه می‌گردد.

## ۹-۱- واژه‌نامه

در این بخش، لغت‌نامه انگلیسی به فارسی (به ترتیب حروف الفبای انگلیسی) و جدول علائم اختصاری قرار داده شده است.

**جدول ۹-۱-۱-۱ لغت‌نامه انگلیسی به فارسی**

| | |
|---|---|
| Accenture | اکسنچر |
| Access technologies | فناوری‌های دسترسی |
| Accountability | قابلیت حسابرسی |
| Actuator | محرک |
| Adelaide | آدلاید |
| Ad-hoc | شبکه اقتضایی |
| Agility | چالاکی |
| Alertme | آلرت‌می |
| Amasa Leland Stanford | لیلند استنفورد |
| Amazon | آمازون |
| analytic | آنالیتیک |
| Any Paradigm | پارادایم "هر" |
| Arduino | آردوینو |
| Arjen Dorland | آرجن دورلند |
| ARM | آرم |
| Arrow Electronics | ارو الکترونیک |
| Asset | دارایی |
| Assurance | اعتماد |
| Autonomy | خودمختاری |
| axeda | آکسدا |
| Azure | آزور |
| Backup | نسخه پشتیبان |
| Base management | مدیریت پایه‌ای |
| Belkin | بلکین |
| Benchmarking | محک زدن |

| | |
|---|---|
| Berkeley | برکلی |
| Big Data | داده‌های عظیم |
| Blackberry | بلک‌بری |
| BlockChain | زنجیره قالب |
| Brighton | برایتون |
| Bundle | مجموعه کامل |
| calAmp corp | کالمپ |
| Cambridge | کمبریج |
| Cincinnati | سینسیناتی |
| Cisco | سیسکو |
| Cleveland | کلیولند |
| Cloud | ابر |
| Common Ground | زمین مشترک |
| Compliancy | پذیرش |
| Connected car | ماشین متصل |
| Connected Health | سلامت متصل |
| Context awareness | آگاهی از محتوا |
| Control4 | کنترل۴ |
| Cross Certification | گواهی‌های متقابل |
| Crowdsourcing | منابع جمعیتی |
| Data breach | نفوذ به داده‌ها |
| Data minimization | کمینه‌سازی داده |
| Data Mining or Forecasting | استخراج یا پیش‌بینی داده |
| Data model | مدل داده |
| Denial of Service | از دست دادن سرویس |
| Digital Catapult Centre | مرکز منجنیق دیجیتال |
| Distributed | توزیع شده |
| Diversity | گوناگونی |
| Echo | اکو |
| Electronic Arts | الکترونیک آرتز |
| Electronic Product Code (EPC) | کد تولید الکترونیکی |
| Embedded Web Resources | منابع وب جاسازی شده |
| End to End | پایان به پایان |
| ENEA | انهآ |
| Energy Efficient Office | دفتر کارایی انرژی |
| Energy Harvesting | استخراج انرژی از محیط |
| Environment | محیط |

| | |
|---|---|
| Ericsson | اریکسون |
| EuroTech | یوروتک |
| Extensible Authentication Protocol | پروتکل احراز هویت توسعه‌پذیر (EAP) |
| Failure | خرابی |
| Fariness | انصاف |
| Feasibility | امکان سنجی |
| Fitbit | فیت‌بیت |
| Fleet management | مدیریت ناوگان |
| Forrester | فورستر |
| fosstrak | فوستراک |
| Fragmentation | تقسیم‌بندی |
| Freshness | تازگی |
| Fudan | فودان |
| Future Proof Designs | طراحی‌ها با تضمین آینده |
| Future Technology Promotion Project | پروژه ارتقای فناوری آینده |
| Gartner | گارتنر |
| Gartner’s Hype Cycle | چرخه هایپ گارتنر |
| Gateway | درگاه |
| Gemalto n.v. | جمالتو ان.وی. |
| General Electric | جنرال الکتریک |
| Georgia Tech | جورجیا تک |
| Goldman sachs | گلدمن ساچز |
| Haier | هایر |
| HANA | هانا |
| Handling | هدایت |
| Harbor Research | هاربورریسرچ |
| Harden | سخت کردن |
| Health monitoring | نظارت سلامت |
| Heathrow | هیترو |
| Helion | هلیون |
| Heterogeneity | ناهمگونی |
| Hewlett-Packard | هیولت پاکارد |
| Hierarchical | سلسله‌مراتبی |
| History | تاریخچه |
| HomeKit | هوم‌کیت |
| HomeOS | سیستم عامل خانه |

| | |
|---|---|
| Host Identity Protocol | پروتکل شناسایی مهمان (HIP) |
| iBeacon | آیبیکن |
| IBM X-Force Research and Development | نیروی تحقیق و توسعه X شرکت IBM |
| Implicit | مطلق |
| Inconvenience | ناسازگاری |
| Information Service Layer | لایه سرویس اطلاعات |
| Infrastructural | زیرساختی |
| Institute | انستیتو |
| Integrated | جاسازی |
| Intel inside | اینتل در داخل |
| Intel R&D centers | آزمایشگاه‌های باز اینتل |
| Interface | رابط |
| Internet of place | اینترنت مکان |
| Internet of Things | اینترنت اشیاء (IoT) |
| Internet of Things and People (IOTAP) | اینترنت اشیاء و افراد |
| Internet of Things foundation | بنیاد اینترنت اشیاء |
| Interoperability | سازگاری |
| Intranet of Things | اینترانت اشیاء |
| InvenSense | اینون‌سنس |
| Jawbone | جابن |
| Juniper | جانیپر |
| Keio | کیو |
| Key Building Blocks | جعبه‌های سازنده اصلی |
| Kinect-base | کینکت-مبنا |
| kit | کیت |
| Kuka | کوکا |
| Leap of Faith | پرش عقیده |
| Lifelogger | لایف‌لاگر |
| Linkedin | لینکدین |
| Living Lab approach | رویکرد آزمایشگاه زندگی |
| Location Privacy | حریم خصوصی مکانی |
| Logistic | منطق |
| LogMeln | لاگملن |
| Long-Tail Product Category | محصولات با دنباله طولانی |
| Looksee | لوک‌سی |
| Low-Power | تراشه‌های کم مصرف |
| M2M | ماشین-به-ماشین |

| | |
|---|---|
| Malmo | مالمو |
| Malware | بدافزار |
| Manageability | مدیریت پذیری |
| Markets&Markets | مارکتس اند مارکتس |
| Massachusetts | ماساچوست |
| Materials | عناصر |
| McGagh | مک گا |
| Mckinsey | مکنزی |
| Medria | مدریا |
| Michigan | میشیگان |
| Middleware | میان‌افزار |
| Mobilitiy | تحرک‌پذیری |
| Modes of Operation | سبک‌های عملیاتی |
| Motorola | موتورولا |
| Myo | میو |
| Nest | نست |
| Network- independent | مستقل از شبکه |
| Networked Radio-Frequency Identification | هویت‌یابی فرکانس-رادیویی شبکه شده |
| Nevigant | نویگنت |
| Non-repudiation | انکارناپذیری |
| Nordic Semiconductor | نوردیک ابررسانا |
| Open community | انجمن باز |
| Open Marketplace | بازار باز |
| Open Source | منبع باز |
| Open User Centred Innovation paradigm | پارادایم نوآوری مرکزی شده کاربر باز |
| Open-source | منبع باز |
| Oracle | اراکل |
| Parkinson | پارکینسون |
| Pevasive | فراگیری |
| Philipps | فیلیپس |
| Philips | فیلیپس |
| Phishing | فیشینگ |
| Photovoltaic | فتوولتائیک |
| Pipeline integrity | یکپارچگی متوالی |
| Predictive Analytics | تجزیه و تحلیل پیشگویانه |
| Pre-integrated | از قبل یکپارچه |

| | |
|---|---|
| Presenters | نمایش‌دهنده‌ها |
| Privacy by Design | حریم خصوصی به وسیله طراحی |
| Private equity | انصاف خصوصی |
| Product lifecycle management | چرخه عمر محصول |
| Productivity | بهره‌وری |
| Protocol for Carrying Authentication for Network Access | پروتکل ایجاد احراز هویت برای دسترسی به شبکه (PANA) |
| Quality of Information | کیفیت اطلاعات (QoI) |
| Radiation | تشعشع |
| Reader | خواننده |
| Real-time | آنی |
| Reliability | قابلیت اطمینان |
| Remote Patients Assitance | کمک از راه دور به بیماران |
| Resilient reputation | اعتباری ارتجاعی |
| Resolution Infrastructure | زیرساخت تفکیک |
| Retail | خرده‌فروشی |
| Revenue | درآمد |
| Rework | دوباره کار انداختن |
| Rio Tinto | ریو تینتو |
| Safeguard Scientifics | سیفگارد ساینتیفیک |
| SAP | سپ |
| Scalability | مقیاس‌پذیری |
| Seamless | بی‌درز |
| Secure handshake | دست امن |
| Security Imprinting | مهر امنیتی |
| Self-configure | خودپیکربند |
| Self-managed | خودمدیریتی |
| Server/client | سرور/کاربر |
| Shell | شل |
| Sierra wireless | سیرا بی‌سیم |
| Silicon | سیلیکون |
| Smart Home Protocol (SHP) | پروتکل خانه هوشمند |
| Software AG | سافت‌ویر ای‌جی |
| Software-defined Hardware | سخت‌افزارهای تعریف شده توسط نرم‌افزار |
| Spam | اسپم |
| St. Gallen | سنت گالن |
| Stanford | استنفورد |

| | |
|---|---|
| Streaming | جریانی |
| Streming | تجزیه و تحلیل جاری |
| Sun Microsystems | سان مایکروسیستمز |
| Supply chain | زنجیره تأمین |
| System Modularity | پیمانه‌ای بودن سیستم |
| Tag | برچسب |
| Tampering | شناسایی نفوذ |
| Technical maturity | بلوغ فنی |
| The European Lighthouse Integrated Project | پروژه اتحاد فانوس اروپا |
| thingworx | سینگورکس |
| Tool Support | پشتیبان ابزار |
| Trust | اعتماد |
| Trust Negotation | مذاکره اعتماد |
| Urbanization | شهری‌سازی |
| Usage Control | کنترل استفاده |
| Validate Against | قانونی کردن |
| Verizon | وریزون |
| Violation | تخطی |
| Virtual Machine | ماشین مجازی |
| Visiongain | ویژن‌گین |
| Wearable | پوشیدنی‌ها |
| Web of globally linked hypermedia | وب ابررسانه جهانی |
| Wellbeing | تندرستی |
| Winning solution | راه‌حل برنده |
| Wisconsin | ویسکانسین |
| Yahoo | یاهو |
| Zebra | زبرا |
| Zürich | زوریخ |

### جدول ۹-۱-۱-۲ علائم اختصاری

| | |
|---|---|
| IPV6 over Low Power Wireless Personal Area Networks | 6LOWPAN |
| Autonomous Decentralized Peer-to-Peer Telemetrya | ADEPT |
| Advanced Malware Protection | AMP |
| Advanced Massage Queuing Protocol | AMQP |
| Architectural Reference Model | ARM |
| Building Radio frequency Identification solutions for Global Environment | BRIDGE |
| Center for Development andApplication of Internet of Things | CDAIT |

| | |
|---|---|
| Constrained Application Protocol | COAP |
| Collaborative Open Market to Place Objects at your Service | Compose |
| Collective Security Intelligence | CSI |
| Dedicated Short Range Communication | DSRC |
| Datagram Transport Layer Security | DTLS |
| Enabling the Buiness-based Internet of Things and Services | Ebbits |
| Experiential Living Lab for the Internet of Things | Elliot |
| The European Technology Platform on Smart Systems Integration | EPoSS |
| European Telecommunication Standards Institute | ETSI |
| IDC | IDC |
| Institute of Electrical and Electronics Engineers | IEEE |
| European Research Cluster on the Internet of Things | IERC |
| Internet Engineering Task Force | IETF |
| Internet of Everything | IoE |
| Korean Advanced Institute of Science and Technology | KAIST |
| Key Exchange Mechanism | KEM |
| Lightweight Local Automation Protocol | LLAP |
| Low Power Wide Area Network | LPWAN |
| eMbedded devices Gateways Cloud | MGC |
| Message Queuing Telemetry Transport | MQTT |
| Managed Threat Defense | MTD |
| Near Field Communication | NFC |
| Organization for the Advancement of Structured Information Standards | OASIS |
| Original Equipment Manufacturer | OEM |
| Open Geospatial Consortium | OGC |
| Object Management Group | OMG |
| Over The Air | OTA |
| Open Web Application Security Project | OWASP |
| People to Machine | P2M |
| People to People | P2P |
| PricewaterhouseCoopers | PWC |
| Representational state transfer | REST |
| Self-serving Asset in Highly  Networked Enviroment | SAHNE |
| Secure Internet of Things Project | SITP |
| Standard Marine Communication Phrases | SMCP |
| Secure Middleware for Embedded Peer-to-Peer | SMEPP |
| Service Oriented Architecture | SOA |
| Simple Object Access Protocol | SOAP |
| Security Research and Operations | SR&O |
| Simple Sensor Interface | SSI |
| Security & Trust Organization | STO |
| Transmission Control Protocol - Internet Protocol | TCP-IP |
| User Datagram Protocol | UDP |
| Vehicle to Infrastructure | V2I |
| Vehicle-to-Vehicle | V2V |
| Web-Oriented Architecture | WOA |
| Extensible Messaging and Presence Protocol | XMPP |

## ۹-۲- مراجع

1. Zhou Book: Internet of things in the cloud, a middleware prespective, Honbo Zhou, 2013
2. everything-for-cities: The internet of everything for the cities, Shane Mitchell et. al.,
3. http://www.gartner.com/newsroom/id/2819918
4. http://www.techtimes.com/articles/31467/20150208/top-5-internet-things-devices-expect-future.htm
5. http://atos.net/content/dam/global/documents/your-business/atos-white-paper-internet-of-things.pdf
6. https://tech.co/internet-of-things-shaping-future-2014-11
7. http://iot-analytics.com/iot-market-segments-analysis
8. http://iot-analytics.com/iot-market-forecasts-overview
9. http://iot-analytics.com/10-internet-of-things-applications
10. Haghighi Report: محمد صیاد حقیقی ,بررسی روند تکاملی اینترنت اشیاء و معماری آینده آن
11. MGI_Disruptive_technologies_Full_report_May2013
12. Create_the_Internet_of_Your_Things_Top_10_Benefits
13. http://iot-analytics.com/iot-infrastructure-providers-iot-hype/
14. IERC Cluster Book
15. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=Manufacturers
16. http://www.theinternetofthings.eu
17. http://iot-analytics.com/15-internet-of-things-stocks
18. http://iot-analytics.com/20-internet-of-things-companies/
19. http://internet-of-things.meetup.com/cities/us/ca/stanford/
20. http://dataconomy.com/stanford-researchers-invent-multistoried-chips-to-address-the-rise-of-iot-and-big-data/
21. http://iot.stanford.edu/people.html
22. http://www.technologyreview.com/news/534506/sniffing-radio-frequency-emissions-to-secure-the-internet-of-things/
23. http://en.wikipedia.org/wiki/University_of_Brighton
24. http://www.digitalcatapultcentre.org.uk/local-centre/brighton/
25. http://en.wikipedia.org/wiki/Malm%C3%B6_University
26. http://web.mit.edu/

27. http://newsoffice.mit.edu/2012/auto-id-cloud-of-things-big-data
28. http://global.mit.edu/projects/project/the-internet-of-things/
29. http://en.wikipedia.org/wiki/University_of_Cambridge
30. http://lsir.epfl.ch/research/current/openiot/
31. http://autoidlabs.org/wordpress_website
32. http://www.iotlab.wisc.edu/about-us.aspx
33. https://labofthings.codeplex.com/documentation
34. http://www.mcafee.com/jp/resources/solution-briefs/sb-intel-gateway-iot.pdf
35. http://www.intel.com/content/www/us/en/internet-of-things/iot-platform.html
36. http://azure.microsoft.com
37. http://www.cisco.com/c/en/us/products/security/index.html
38. http://www.ibm.com/software/products/en/messagesight
39. http://www.ibm.com/security/xforce/
40. http://www.businesskorea.co.kr/article/6149/samsung%E2%80%99s-future-projects-samsung-selects-10-new-research-items-future-growth
41. http://cloudtimes.org/2015/01/21/intel-samsung-cisco-launches-iotivity-open-source-standard-for-the-internet-of-things
42. http://www.rethinkresearch.biz/articles/ibm-samsung-unveil-adept-blockchain-proof-concept-iot-security
43. Internet of things security architecture, Noel Poore, Architect, Java Platform Group, September 29, 2014
44. https://mbed.org/
45. http://www.elliot-project.eu
46. http://www.utrustit.eu
47. http://www.smartie-project.eu/project.html
48. http://www.iot-a.eu/public
49. B. Mandler, Final COMPOSE architecture document, IBM & European Commission, 2014.
50. http://www.iot-butler.eu/about-butler
51. http://iot.stanford.edu/seminar/sitp-w15-sap.pdf
52. http://www.iot-butler.eu/about-butler
53. IJCN-265: Towards Internet of Things: Survey and Future Vision, O. Said, M. Masud, International Journal of Computer Networks (IJCN), Vol. 5, Issue 1, 2013
54. http://www.gartner.com/it-glossary/web-oriented-architecture-woa

55. T. H. Miguel Blockstrand, lars-Örjan kling, Robert Skog and Berndt Wallin Operator opportunities in the internet of things, Ericsson review, 2011.