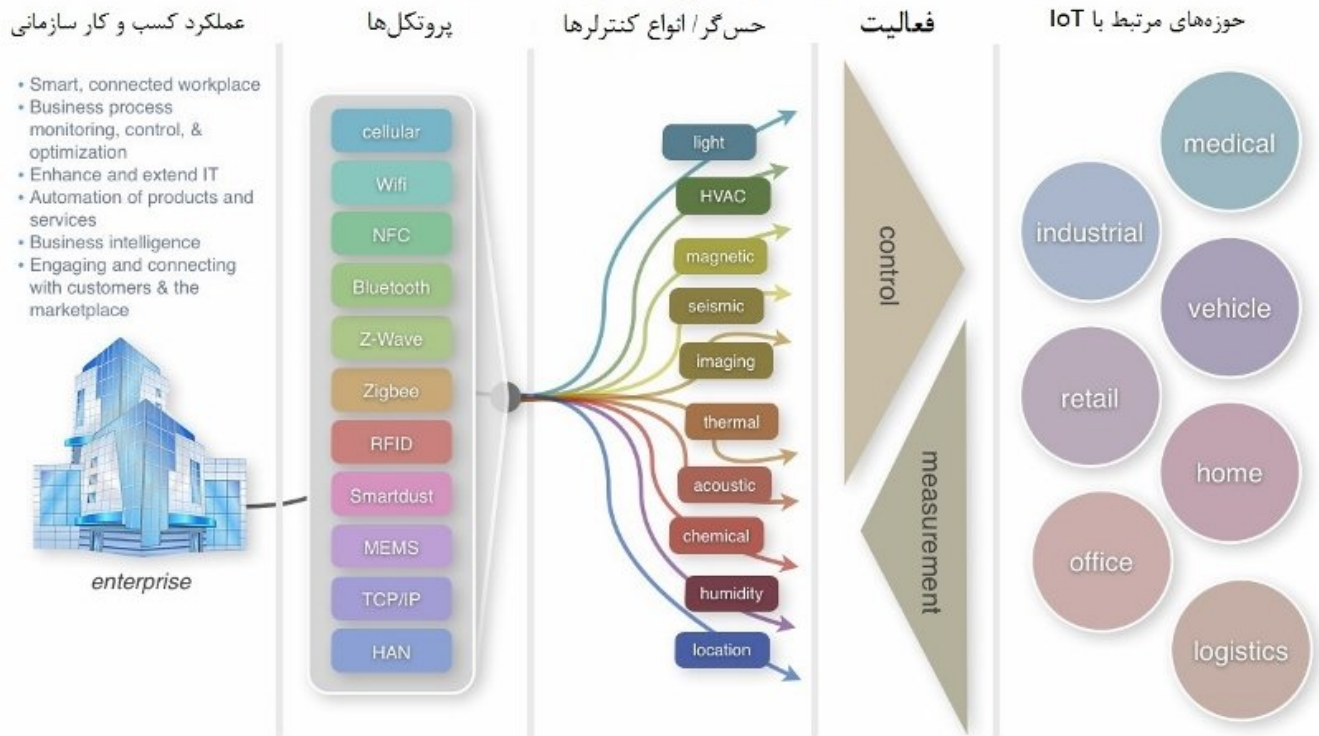




# نمای سازمانی اینترنت اشیا



From <http://zdnet.com/blog/hinchcliffe> on ZDNet.

1: ... ..

## اتحادیه اروپا از متولیان ارائه معماری اینترنت اشیا

هدف پروژه اتحادیه اروپا تحت عنوان SENSEI، ایجاد معماری باز کسب‌وکارمحور است که به مشکلات مقیاس‌بندی برای تعداد گسترده‌ای از دستگاه‌های WS & AN توزیع شده در سراسر جهان اشاره می‌کند. برای عملی ساختن راه‌حل‌های استاندارد RFID و EPCGlobal باید بر محدودیت‌های فنی، اجتماعی و آموزشی فائق آمد. BRIDGE (سرنام Building Radio Frequency Identification solutions for the Global Environment) به معنای ایجاد راه‌حل‌های شناسایی از طریق فرکانس رادیویی برای محیط جهانی، از طریق توسعه معماری شبکه EPC به این مشکلات اشاره می‌کند. این امر از طریق تحقیق، توسعه و اجرایی کردن ابزارهایی که به گسترش برنامه‌های کاربردی EPCGlobal در اروپا منجر خواهد شد، تحقق می‌پذیرد. این گسترش غالباً مشروط به توسعه دستگاه‌های امنیتی، سخت‌افزاری، نرم‌افزاری و توسعه تعالیم کسب‌وکار است.

## پروژه CUBIQ

هدف پروژه CUBIQ (سرنام The Cross Ubiquitous Platform) به معنای پروژه پلتفرم سراسری متقابل، ایجاد پلتفرمی مشترک است که توسعه برنامه‌های کاربردی متن‌آگاه را آسان‌تر سازد. این ایده بر آن است تا پلتفرمی یک‌پارچه را ایجاد کند که ارائه‌دهنده خدمات و پردازش دسترسی به داده‌های یک‌پارچه است.

## معماری CUBIQ

CUBIQ شامل سه لایه زیر است:

- 1- لایه منبع داده‌ها: دسترسی و اداره شفاف داده‌ها را فراهم می‌سازد و پویایی، جابه‌جایی، تکرار، خطاها و پایداری داده‌ها را مدیریت می‌کند.
  - 2- لایه پردازش‌گر درون‌متنی: ارائه‌دهنده خدمات پردازش داده است.
  - 3- لایه پردازش‌گر برون‌متنی: مسئولیت ترکیب خدمات را بر عهده دارد.
- معماری CUBIQ رابط‌هایی را برای هر لایه ایجاد می‌کند. علاوه بر نتایج به دست آمده از تلاش‌های تحقیقاتی، چند معماری وجود دارد که اکنون در چند محصول تجاری مورد استفاده قرار می‌گیرد.

## محصولات تجاری

### Zigbee

توسط اتحاد زیگبی ایجاد شده و ظاهراً محبوبترین پروتکل است. اما چرا؟ به دلیل این که جایگزین ساده‌تر و قابل‌قیاس‌تری نسبت به بلوتوث است. زیگبی پروتکل ارتباطی برای لایه کاربردی به شمار می‌رود. برنامه‌هایی که به نرخ دسترسی پایین داده‌ها، عمر بالای باتری و شبکه ایمن احتیاج دارند، از این پروتکل استفاده می‌کنند. این پروتکل نخستین بار در سال 2004 معرفی شد و از آن زمان تاکنون به‌روزرسانی‌های متعددی روی آن اعمال شده است.

### Wireless HART

محصول توسعه یافته و محبوب فناوری ارتباطی HART است. HART (سرنام Highway Addressable Remote Transducer) به معنای مبدل از راه دور و نشانی‌پذیر بزرگراه است. این محصول ویژگی‌هایی همچون امنیت و دوام دارد، اما به دلیل فلسفه تک‌منظوره خود فاقد قابلیت به اشتراک‌گذاری داده‌ها با دیگر فناوری‌های ارتباطی است. از جمله ویژگی‌های شاخص این پروتکل به موارد زیر می‌توان اشاره کرد:

- برقراری ارتباط با دستگاه‌ها در یک میدان از طریق فرآیند هوشمند
- توسعه یافته از فناوری ارتباطی محبوب Wired HART برای برنامه‌های بی‌سیم
- پیاده‌سازی بر مبنای استاندارد IEEE 802.15.4-2006 PHY و پشتیبانی‌کننده از نشانی‌های مک
- قابلیت پیاده‌سازی ارتباطات بی‌درنگ از طریق مدیریت مرکزی شکاف‌های TDM و مسیریابی شبکه‌های مش (Mash)
- پیاده‌سازی ارتباطات ایمن از طریق مکانیسم‌های ارتباطی امنیتی

### Sun SPOT

پلتفرمی از شرکت Sun Microsystems است که به‌منظور توسعه شبکه‌های حس‌گر و سیستم‌های نهفته ایجاد شده است. Sun SPOT (سرنام Sun Small Programmable Object Technology) به معنای فناوری شیء قابل برنامه‌ریزی کوچک سان است. بر عکس دیگر سیستم‌های توکار، توسعه این سیستم بر مبنای زبان سی‌سی پلاس پلاس یا انشعاب‌های مختلف سی نبوده و با استفاده از زبان برنامه‌نویسی جاوا پیاده‌سازی شده است. بر همین اساس، شرکت سان اقدام به پیاده‌سازی ماشین مجازی خود موسوم به Squawk-VM کرده است. Squawk-VM از جزئیات سخت‌افزار انتزاعی برای دسترسی به ماژول‌های ارتباطی بی‌سیم و حس‌گرهای مختلف استفاده می‌کند. از این رو، پیاده‌سازی کامل برنامه‌ها بر مبنای Sun SPOT به‌سادگی انجام می‌شود. گره‌های حس‌گر توانایی به‌کارگیری چند وظیفگی به معنای اجرای چند وظیفه و چند پردازشی به معنای اجرای چند برنامه را دارند. مدل ارتباط Sun SPOT بر مبنای استاندارد IEEE 802.15.4 ساخته شده است.

### Representational State Transfer

REST نمایان‌گر حالت انتقال (سرنام Representational State Transfer)، مجموعه‌ای هماهنگ از فیدهای معماری است که برای به حداقل رساندن زمان تأخیر و ارتباط شبکه‌ای تلاش می‌کند و هم‌زمان با آن، وابستگی نداشتن و قابلیت مقیاس‌بندی، پیاده‌سازی اجزا را به حداکثر می‌رساند. این امر با اعمال محدودیت‌هایی روی معناشناختی کانکتور تحقق می‌یابد، در حالی که دیگر روش‌ها روی معناشناختی جزء متمرکز شده‌اند.

REST برای برآورده ساختن نیازهای یک سیستم ابررسانه‌ای توزیع شده در اینترنت، ذخیره‌سازی موقت و استفاده مجدد از فعل و انفعالات، جایگزینی پویای اجزا و پردازش انفعالات توسط واسطه‌ها را ممکن می‌سازد. REST تنها آن بخش‌هایی از معماری را با جزئیات توصیف می‌کند که برای تعامل ابررسانه‌ای توزیع شده در مقیاس اینترنت ضروری به نظر می‌رسد. با توجه به پروتکل‌های ارتباطی، چند راه‌حل به‌منظور غلبه بر محدودیت‌های فناوری‌های شبکه‌ای کنونی ایجاد شده است.

### پروتکل‌های ارتباطی

پروتکل انتقال کنترل جریان SCTP

SCTP پروتکل استاندارد پیشنهادی IETF برای لایه انتقال است. این پروتکل طراحی شده است تا در نهایت جایگزین TCP و شاید UDP شود. SCTP همانند پروتکل TCP معتبر و قابل اطمینان است، اما ویژگی‌های جدیدی همچون چندجریانی (Multi-Streaming) و پشتیبانی از چند فضا (Multi-Homing) را ارائه می‌دهد. ویژگی پشتیبانی از چند فضا SCTP را قادر می‌سازد تا برای پشتیبانی از جابه‌جایی در شبکه، به هیچ عامل اختصاصی روتر در شبکه نیازی نداشته باشد. از دیگر ویژگی‌های موجود در پروتکل SCTP می‌توان به انتقال داده‌ها به‌صورت غیر تکراری و بدون

خطا، تحمل‌پذیری خطا در سطح شبکه از طریق ویژگی پشتیبانی از چند فضا و مقاومت در برابر حملات جعل هویت و حملات طوفانی اشاره کرد.

## پروتکل هویت میزبان HIP

HIP راه‌حلی است که حرکت و جابه‌جایی میان شبکه و لایه‌های انتقال را موقعیت‌یابی می‌کند. HIP لایه هویت میزبان جدیدی (لایه 5/3) را بین لایه‌های IP و لایه‌های بالایی معرفی می‌کند. دلیل این امر اجتناب از موقعیتی است که در آن متصل کردن سوکت‌ها به IP نشانی‌ها، نشانی را به ایفای نقش دوگانه شناساگر نقطه پایانی و شناساگر ارسال وادار می‌سازد. در HIP، سوکت‌های لایه‌های بالایی به جای IP نشانی‌ها به هویت‌های میزبان (شناساگرهای HIP) متصل می‌شوند. علاوه بر این، اتصال این هویت‌های میزبان به IP نشانی‌ها (موقعیت‌یابی‌ها) به‌طور پویا صورت می‌گیرد. هدف HIP پشتیبانی از اعتماد میان سیستم‌ها، افزایش حرکت و جابه‌جایی و کاهش چشم‌گیر حملات محروم‌سازی از سرویس (DOS) است.

## پروتکل IP

پروتکل IP موبایل استاندارد پیشنهادی از سوی IETF است که راه‌حل مرتبط با لایه شبکه را برای تحرک و جابه‌جایی گره در سراسر شبکه‌های IPv4 ارائه می‌دهد. IP موبایل به یک گره این امکان را می‌دهد تا نقطه اتصال خود به اینترنت را بدون نیاز به تغییر IP نشانی خود تغییر دهد. این امر صرفاً برای ساده‌سازی تنظیمات انجام نمی‌پذیرد، بلکه در هنگام جابه‌جایی گره از نقطه‌ای به نقطه دیگر موجب آسان‌تر شدن اتصال مستمر در سطح برنامه کاربردی می‌شود. با استفاده از IP موبایل، جابه‌جایی یک دستگاه تک‌آی‌پی در اینترنت بدون از بین رفتن اتصال در سطوح بالایی امکان‌پذیر است. هر چند با تکثیر و ازدیاد IP و امید به اتصال مدام به اینترنت این احتمال وجود دارد که بتوان حرکت و جابه‌جایی تمام این دستگاه‌ها را با استفاده از IP موبایل استاندارد ممکن ساخت، اما این امر مستلزم آن است که تمام دستگاه‌ها گنجایش IP موبایل را داشته باشند و بار اضافی ایجاد نکنند، به گونه‌ای که هر دستگاه وظایف IP موبایل خاص خود را انجام دهد. راه‌حل دیگر برای این مسئله تحرک و پویایی شبکه (NEMO) است که از طریق جابه‌جایی، قابلیت حرکت از گره‌های متحرک 3 موبایل به روتر شبکه را امکان‌پذیر می‌سازد. روتر قادر است نقطه اتصال خود به اینترنت را به گونه‌ای تغییر دهد که برای گره‌های متصل شده روشن و شفاف به نظر برسد.

## NEMO، پروتکل توسعه یافته IP

NEMO شکل توسعه یافته IP موبایل است که کل یک شبکه را قادر می‌سازد تا نقطه اتصال خود به اینترنت را تغییر دهد. در حیطه اینترنت اشیا، اشیای هوشمند و خدماتی که از آن‌ها بهره می‌برند در سراسر جهان پراکنده شده‌اند. از این رو، باید نوعی زیرساخت شناسایی و تفکیک به‌منظور کشف و تکیه بر خدماتی که امکان دسترسی به اطلاعات پیرامون اشیا هوشمند و همچنین کنترل آن‌ها را میسر می‌سازند، وجود داشته باشد. ضرورتاً، شناسایی منبع می‌تواند هم دربردارنده نام‌گذاری و هم نشانی‌دهی یک منبع یا یکی از آن‌ها باشد. در وب، شناسایی منبعی که نمایان‌گر شکلی از اطلاعات باشد، از طریق ایجاد «شناسه منابع جهانی» (URI) که قراردادی جهانی پیرامون شناسایی منبعی خاص بر اساس طرح‌هایی مشخص است، صورت پذیرفته است. در اینترنت اشیا همانند اینترنت و وب، اشیا و منابع باید طرح‌های کلی نام‌گذاری و نشانی‌دهی مشترک و همچنین خدمات شناسایی داشته باشند تا امکان دستیابی جهانی به آن‌ها را امکان‌پذیر سازد. در پروژه SENSEI، شناسه منبع از طریق به هم پیوستن چند پارامتر زیر ایجاد می‌شود:

- دامنه ارائه‌دهنده منبع

- نوع دستگاه

- نامی نشان‌دهنده عملکرد منبع

- در نهایت، شناساگر منحصر به فرد و خاصی که منبع را از دیگر اجزا متمایز می‌کند.

در شناسه سراسری (UID)، شناسایی چهارچوب کار توسط «کد u» که شناساگری منحصر به فرد برای ماهیت‌های فیزیکی یا منطقی است، ارائه می‌شود. کد u عددی 128 بیتی است که هیچ گونه رابطه‌ای با آن‌چه نشان می‌دهد ندارد و در عوض، این رابط از طریق سرورهای پایگاه داده اختصاصی بازبایی می‌شود. ساختار کد u به گونه‌ای شکل گرفته است که از مدیریت خودمحوری پشتیبانی کند. در زمینه شناسایی از طریق فرکانس رادیویی، RFID، EPCGlobal، به‌کارگیری و استانداردسازی کد الکترونیکی محصول (EPC) را که صرفاً به عنوان ابزاری در جهت شناسایی برچسب‌های RFID مورد استفاده قرار می‌گیرد، ارتقا بخشیده است. این کد بر اساس مدل URI است. ID@URI که از طریق پروژه تحقیقاتی DIALOG ایجاد شد نیز مدل شناسایی دیگری است که همان ویژگی‌های استاندارد EPC/ONS را دارد، اما علاوه بر آن، می‌تواند در بارکدها نیز نمود داشته باشد.

## ناهماهنگی در مؤلفه‌های کلیدی معماری

از هر زاویه‌ای که به موضوع بنگریم، نیازمند پیش‌رفتی اساسی در این زمینه هستیم. در ابتدا، باید گفت امروزه برای شناسایی یک شیء در اینترنت اشیا، هیچ راه مشخصی وجود ندارد. چند استاندارد نظیر بارکدهای دوبعدی، UID، GS1، IPv6، نشانی‌ها وجود دارند، اما ناسازگار هستند. افزون بر این، معماری‌های مرجعی که می‌توانند موجب پیاده‌سازی و اجرای هر گونه سیستم واقعی شوند، باید شناسایی و استانداردسازی شوند. همچنین، مکانیسم‌های امنیتی باید تضمین‌کننده ویژگی‌های امنیت و حریم خصوصی مناسب باشند. پروتکل‌های ارتباطی از لایه فیزیکی گرفته تا رابط‌های خدمات و برنامه‌های کاربردی برای افزایش هر گونه دید و آگاهی نسبت به اینترنت اشیا در آینده‌ای نزدیک به پیش‌رفت‌هایی اساسی نیاز دارند. نمونه‌های بالا تنها موارد کمی از زمینه‌های تحقیقاتی هستند که در پنج تا ده سال آینده نیاز به پیش‌رفت اساسی دارند. در حیطه اینترنت اشیا که با اشیا سروکار دارد، لزوم پیاده‌سازی هم‌گرایی میان وسایل ارتباطی مختلف امری ضروری و اجتناب‌ناپذیر است. امروزه چند مکانیسم ارتباطی مختلف در برنامه‌های کاربردی مورد استفاده قرار گرفته‌اند، اما تمام فناوری‌های نوین باید به‌اشتراک‌گذاری داده‌ها میان پروتکل‌های مختلف را تضمین کنند. همچنین، باید در نظر داشته باشیم که طول عمر فناوری‌های شبکه‌ای ممکن است بسیار کوتاه‌تر از اشیا فیزیکی متصل به شبکه باشد. در اینترنت «معمولی»، اشتراک داده‌ها میان فناوری با لایه‌های پایین و خدمات با استفاده از پروتکل اینترنتی (IP) تضمین می‌شود. معمولاً فناوری‌های شبکه به شکل ساعت شنی نمایش داده می‌شوند، به گونه‌ای که لایه IP در وسط قرار می‌گیرد که اصطلاحاً به‌عنوان «کمر باریک» اینترنت اطلاق می‌شود. پرسش‌هایی نظیر این‌که «کمر باریک» اینترنت اشیا چه شکلی خواهد داشت و این‌که با توجه به نامتجانس بودن فناوری‌های اینترنت اشیا، آیا چنین چیزی وجود خواهد داشت یا خیر، از اهمیت ویژه‌ای برخوردار است و تحقیقات آینده نیز باید به گونه‌ای مشخص بر این موضوع متمرکز شوند. با توجه به مسائل امنیتی اشیا ارتباط برقرارکننده، تاکنون تحقیقات عظیمی پیرامون پیاده‌سازی رمزنگاری مناسب برای دستگاه‌های کم‌هزینه با توان عملیاتی پایین و محدود از نظر منابع صورت گرفته است. این تحقیقات تحت عنوان «رمزنگاری سبک وزن» نامیده شده و توانسته است تعدادی پروتکل جدید را برای دستگاه‌های کوچک همانند برچسب‌های RFID تولید کند. با وجود تعداد زیاد روش‌های موجود، تنها تعداد بسیار کمی از آن‌ها به اندازه کافی مورد بررسی قرار گرفته و ایمن تلقی شده‌اند. در سال‌های گذشته، ثابت شد تعدادی از الگوریتم‌های رمزنگاری سبک وزن که به‌طور گسترده مورد استفاده قرار گرفته‌اند، نفوذپذیر بوده‌اند. الگوریتم شناخته شده MiFare Crypto-1 نمونه‌ای از این الگوریتم‌های نفوذپذیر است. توسعه استانداردهای رمزنگاری سبک وزن برای استفاده گسترده در فناوری‌های اینترنت اشیا حائز اهمیت است. علاوه بر این، ترکیب پروتکل‌های رمزنگاری سبک وزن برای استفاده در دستگاه‌هایی که برای کارهای سبک طراحی شده‌اند و چهارچوب رمزنگاری عادی از قبیل زیرساخت کلید عمومی (PKI) برای زیرساخت‌های پایانی باید مورد تجزیه و تحلیل قرار گیرند. نکته بسیار مهمی که باید در این باره مد نظر قرار گیرد، مدیریت کلید است. در چنین چهارچوب‌های کلی‌گرایانه‌ای باید عوامل تولید کلیدهای رمزنگاری عمومی/خصوصی و این‌که چگونه این کلیدها در شبکه توزیع شده و در مواقع ضروری به چه کسی (کدام آژانس‌ها، شرکت‌ها و مقامات مسئول) اجازه دسترسی به چنین کلیدهایی را ارائه می‌کنند، شناسایی شوند.

تاریخ انتشار:

24 آبان 1394