API Management for the Internet of Things (IoT)

A fundamental premise of the Internet of Things (IoT) is the recognition of a certain human weakness. Humans are poor data collectors. We are poor fact collectors. We are poor sensors. Our senses fail us, we make mistakes, and we misremember. Research in Psychology shows that our brains fill-in fragmented memories with phantom events and facts when we can't remember what really happened. Far too often facts are colored by our own value judgments and biases. Worse, we have limited time to focus on fact collecting, so what we get in sum total is a weak representation of the information available to us, especially information in digital form on the Web and throughout the Internet. As good as the web is, it's *weak information* compared to the potential. Why is it weak? It's weak because we typed most of it in.

But I'm a smart thing that talks APIs!
(Image courtesy of JD Hancock
under the creative commons license)

Human mediated information is a slow-path recipe for inefficiency, at least compared to the promise of the Internet of Things (IoT) where full-time Internet-linked sensors and devices with perfect accuracy and a tireless work ethic make a far better substitute. Sensing data timely and accurately, however, is only half of the battle. Data needs to make it into existing back-end systems, fused with other data sources, analytics and mobile devices and be made available to partners, customers and employees.

Even more importantly, sensed data needs to arrive with the appropriate contextual information and filtering. If every "thing" out there has a sensor and is providing data with regular frequency, it's not feasible to process data from all sensors at all times, so we need contextual filtering and way to direct attention to the relevant data that we care about as well as behave properly in the face of failures and spontaneous reconfiguration of the sensor node network. **In short, we need *things-as-a-service (TaaS).*** How can we get there? API Management.

API Management Holds the Key

This is precisely where Web APIs, API Management and a RESTful architecture provide dramatic value. As APIs have become ubiquitous, IoT deployments in a wide range of market segments can benefit from this proven architecture. **APIs lower the barrier to entry for connectedness and enable secure communication from sensor nodes to applications living just about anywhere – in any cloud, any datacenter or accessible from API-enabled devices**. Moreover, RESTful communication has well-defined security patterns for bulletproof API management, including authentication, authorization, leak protection, compliance and data security. If you can get your "thing" to talk APIs you've got a back-stage pass to the the party, so to speak.

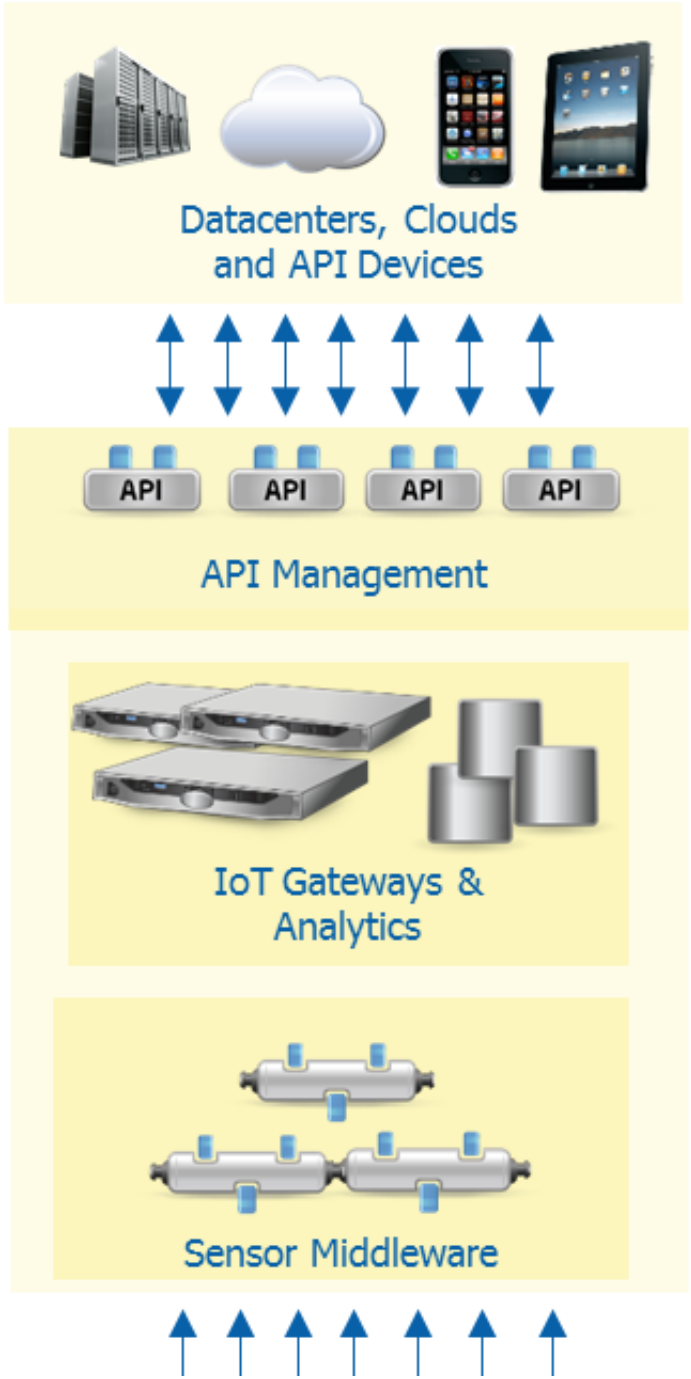
API Devices or Sensors

In the context of APIs and IoT, it makes some sense to talk about the distinction between sensors and devices. First off, everything is a thing, but some of the members in the Internet of things are *already* API-enabled and some are not.

Some *things* can already provide contextual information from its environment and some cannot. Most notably HTML5 & native smart-phones and tablets are API enabled, whereas a temperature sensor on a factory floor connected via a wireless sensor network (WSN) is not.

If you have sensor nodes in participating in a flat or two-tier sensor network, you aren't really doing IoT unless you can get your data to higher end computational devices. In these so called *brown field* deployments, sensors may be working in complete isolation. With a smart device on the other hand, sensors are coupled to a device that already speaks Web APIs, let's call these *API devices*. Without APIs your sensors are stranded, shouting continuous or discrete data into the 'ether' and getting brown field sensors to join the IoT requires a bolt-on approach or technology bridge to speak APIs. The opposite, *green field* deployments build sensor networks with IoT in mind from the beginning, potentially lowering API on-ramping costs. In either case, brown or green, an intermediate layer is needed to connect *south-side* sensors and networks to *north-side* APIs, clouds, datacenters and devices.

API Management Gateways and Sensor Middleware



API Management and Internet of Things – Conceptual Architecture

This is where sensor middleware and API Management for IoT gateway solutions play an important role: they provide data fusion, contextual information, data communication, coordination & synchronization, data & protocol interoperability, privacy & security, and fault tolerance.

In fact, middleware and gateway technology is far from optional: **The lack of an effective coordination layer has the potential to kill IoT dead in its tracks**. With an extremely large number of sensors undergoing constant chatter, integration costs will be far too high unless organizations rely on proven, well-established communication paradigms such as APIs, and well-understood coordination patterns. On the the other hand, as more things are connected through middleware, this means more data is available, which as a positive impact on apps that use APIs. This virtuous cycle illustrates the power of complements – **more Internet connected things-as-a-service (TaaS) drive increased adoption of APIs which reinforces the IoT vision**. In this sense, middleware and gateways are the great enabler of IoT.

In the conceptual architecture shown in the diagram, sensor networks communicate with *sensor middleware* which can be thought of as one step closer to the raw sensor behavior compared to the gateway. In some cases the gateway itself may subsume all functions of the sensor middleware, depending on the use case. For example, if sensors are enabled with higher level protocols such as CoAP these nodes and networks may be able to talk directly to the gateway itself.

Sensor middleware typically provides the following key capabilities:

1. **Abstraction support** – The ability to provide a homogenous and holistic view of a sensor network in the face of substantially different

sensor hardware and capabilities

2. **Data fusion & enrichment** – The ability to enrich data from sensors with environmental and contextual information, forming a higher level view of the data suitable for consumption by other applications.
3. **Dynamic network** – If sensors are added, moved or removed, sensor middleware must be able to deal with ad hoc changes in the underlying network topology with graceful impact to higher level services
4. **Scalability** – When dealing with a large number of sensors, middleware should have long reliable operation with a potentially large number of sensors
5. **Security** – If sensors are deployed collecting sensitive information, data protection schemes and encryption are required. This is further challenged by the fact that sensors can be low power with low compute capabilities
6. **Network Delivery & Quality of Service** – Maintain consistent availability and behavior in the face of high latency, network failures and bandwidth challenges

Sensor middleware, however, is typically not enough for a managed API suitable for use by the Enterprise, other back-office applications, and smart-devices. Here you need to add a second layer of API management gateways that can provide further value to the data.

API Management and IoT Gateways

API management completes the square for IoT. Gateway, hybrid and SaaS offerings provide the face of communication for raw sensor networks with robust, managed interfaces able to speak to any other API out there, providing universal communication. For IoT specifically, there are a number of other capabilities that gateway technology contributes to the Internet of Things (IoT):

1. **Complete Context** & **Orchestration-** Context for a sensor is any information that characterizes its situation. Complete context opens up sensor data to data from other APIs, application, services, social networks and devices. IoT Gateways provide the ability to mash-up and orchestrate data across any API to bring higher level information to the application, especially from other sensor networks
2. **Adaptive Analytics & Big Data –** Sensors are poised to generate a 10-fold increase in data over the next 5-10 years. IoT Gateways bring well-defined secure interfaces to large scale data sets stored in big data repositories, enabling insights and access to other APIs, applications and devices.
3. **Compliance and Privacy** – IoT Gateways form the control point for data protection. As data is made available through APIs, gateways provide selective data encryption, tokenization, and leak protection, helping to protect privacy and ensure compliance. Even if data cannot be protected at the sensor level, it can be protected at the API level, enabling and enhancing security.
4. **Multi-Tenancy –** The only way shared services required for connected sensor networks can be offered is if there is a shared multi-tenant API management layer on which different developer ecosystems can land as tenants using the same sensor data in different ways. A ‘silo’ approach compromises the developer experience data availability. Without multi-tenancy data enriched by other developer ecosystems unavailable.

5. **Protocol & Data Brokering** – Data from sensor middleware may come over different formats and protocols, ranging from unstructured binary data, semi-structured data and structured data. Sensors may also talk directly to IoT gateways using raw TCP protocols. IoT gateways need to act as a protocol & data consolidation point, aggregating data from other APIs, enterprise systems and across disparate sensor networks to publish secure HTTP(S), Websockets and OAuth 2 enabled APIs to consuming devices.
6. **Onboarding and Discovery** – If nobody knows about your data or your API, how can it ever be used? The use of a developer facing API catalog with self-service capabilities shortens the time to market and makes APIs that include sensor-derived data available to the widest possible developer audience, either public, partner or internal developers.

How about some real-world examples? Most notably we made raw sensor information available through APIs to an HTML5 enabled mobile device here at Intel.

See Travis's blog on the IoT project entitled citizen Developers Empowered by APIs and HTML5. It uses room sensors to maximize the use of conference space and is a great example of APIs and IoT reinforcing each other. This demo required the use of data fusion, scalability, data availability, security, and governance. If you are thinking about an IoT Gateway, check out the Intel(R) Expressway API Management product, which can help enable your IoT vision.

Expressway API Manage Enables API Management for the Internet of Things

"Thing" Image is covered under this creative commons license courtesy of JD Hancock

The post API Management for the Internet of Things (IoT) appeared first on Application Security.