Gartner.

G00296351

Top 10 IoT Technologies for 2017 and 2018

Published: 22 January 2016

Analyst(s): Nick Jones

This research discusses 10 technologies that will be vital for organizations to unlock the full potential of the IoT as part of their digital business strategies.

Key Findings

- The Internet of Things (IoT) demands a wide range of new technologies and skills that many organizations have yet to master.
- A recurring theme in the IoT space is the immaturity of technologies and services and of the vendors providing them. Architecting for this immaturity and managing the risk it creates will be a key challenge for organizations exploiting the IoT.
- In many technology areas, lack of skills will also pose significant challenges.

Recommendations

- Use techniques such as layering and modularity to architect for change so that future developments in technologies or vendors can be accommodated. Modularity may extend to hardware as well as software.
- Evaluate IoT technologies using Gartner Hype Cycles and Market Guides to assess their maturity and risk and to create roadmaps for IoT solutions to transition from tactical to more strategic technologies.
- Catalog the IoT skills gaps in your organization, and train staff or find appropriate partners to address them.

Table of Contents

List of Tables

Analysis

For many organizations, the IoT will be a cornerstone of their digital business strategies, but it will also be very disruptive, requiring them to master many new technologies and capabilities. The technologies and principles of IoT will have a very broad impact on organizations. They will affect business strategy, risk management and a wide range of technical areas such as architecture and network design.

This research discusses 10 IoT technologies that are likely to be on every organization's radar. These are certainly not the only important IoT technologies — Gartner advises organizations to consult its IoT Hype Cycles for details of many more — but these were selected on the basis of their importance to a wide range of organizations and IoT solutions. This note focuses on those technologies that are specific to the IoT; many IoT solutions will also use a wide range of conventional IT technologies that are not discussed here.

The IoT is a very immature domain where product and technology categories aren't yet clearly established, so some of the topics discussed here are less specific technologies than key technology areas that can't yet be satisfied by any single product or vendor. In several cases, it's likely that researchers will develop new technologies and solutions that don't yet exist. One of the recurring themes in these technology descriptions is risk and immaturity. Organizations needing solutions in the short term can't afford to wait until the IoT is mature, so managing vendor and technology risk will be vital to successful IoT deployments. Key principles will include architecting for change — for example, modularizing designs so that software and even hardware technologies can be replaced when superior options emerge.

IoT Security

What is it, and why is it important? The IoT introduces a wide range of new security risks and challenges to the IoT devices themselves, their platforms and operating systems, their communications, and even the systems to which they're connected (such as using IoT devices as an attack channel). Creating smarter products often removes traditional architectural barriers; for example, critical car systems are now exposed to mobile apps (see Note 1 for selected examples of recent IoT security flaws). Security technologies will be required to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications, and to address new challenges such as impersonating "things" or denial-of-sleep attacks that drain batteries. IoT security will be complicated by the fact that many "things" use simple processors and operating systems that may not support sophisticated security approaches.

When? Many security tools and technologies are available in 2016 — although seldom from one single vendor — and often, many aren't well-adapted to current IoT use cases. It's likely that hardware and software advances will make IoT security a fast-evolving area through 2021. Also, some "things" may be long-lived, allowing attackers many years to find vulnerabilities, so security strategies and technologies must be flexible and able to evolve as new threats emerge during a product's lifetime. New approaches and technologies will emerge to provide new types of solutions (see Note 2).

Who will be impacted? Any organization delivering or using the IoT. All roles involved in delivering IoT solutions, including chief information security officers (CISOs), architects, designers and programmers, must become familiar with IoT risks, security principles and technologies. Organizations must review the security used in the IoT systems they purchase as well as those they develop internally.

Cautions: Experienced IoT security specialists are scarce, and in 2016, security solutions are fragmented and involve multiple vendors. New threats will emerge through 2021 as hackers find new ways to attack IoT devices and protocols, so long-lived things may need updatable hardware and software to adapt during their life span. Technology cannot address all security issues; many IoT security problems are related to lack of knowledge resulting in poor design and implementation. Often, the weakest link in IoT security will be people.

IoT Analytics

What is it, and why is it important? IoT business models will exploit the information collected by "things" in many ways — for example, to understand customer behavior, to deliver services, to improve products, and to identify and intercept business moments. However, IoT demands new analytic approaches:

- As we evolve to a future with tens of billions of connected "things," the volume of data to be analyzed will increase dramatically. This creates problems of scale that will be partly addressed by new platforms (see the Event Stream Processing section). But it also means that there will not be sufficient staffing or time for human data scientists to analyze the information. This will demand technologies such as machine learning to identify patterns, which is an area where vendors such as Google and IBM have made major investments.
- The traditional IT approach to data analytics has been to collect and store data, then analyze it. However, in an IoT context, this is not always desirable or practical, so new analytics architectures are emerging. First, there may be too much data to store, so analysis of data

streams must be conducted on the fly. Second, data filtering and analysis may sometimes be distributed in gateways at the edge of the network or in the "things" themselves to minimize communication over slow networks or when communications have undesirable side effects, such as increasing battery consumption in sensor nodes.

- The data collected from "things" may involve new data types and analysis algorithms. Time series data is very common, demanding filters and Fourier transforms. A growing range of "things" are location-aware, demanding geographic information processing.

IoT analytics therefore needs new tools such as high-volume event stream platforms, the ability to operate on new data types, new technologies such as machine learning, and new architectures where analytics is distributed throughout the network of things.

When? New analytic tools and algorithms are needed now, but as data volumes increase through 2021, the needs of the IoT may diverge further from traditional analytics.

Who will be impacted? Data scientists, business intelligence staff, and statisticians performing business analytics will be impacted. Business strategists must be able to exploit new insights and react more rapidly to insights. Network designers must plan for new traffic patterns.

Cautions: Traditional business intelligence and analytics staff may lack skills in areas such as streaming analytics and time series data. As IoT devices proliferate, analytics will be able to generate very personal insights (for example, from monitoring the smart home), so data privacy and acceptable use will become major challenges. Analytics will pose business challenges around data access and ownership; for example, is the data from a ship's engine the property of the ship owner or the engine manufacturer?

IoT Device (Thing) Management

What is it, and why is it important? Long-lived nontrivial "things" will require management and monitoring. This includes device monitoring (for example, are devices still alive, are they connected, and what is their battery status?), firmware and software updates, diagnostics, crash analysis and reporting, physical management (for example, installation, retirement and relocation of things), and security management. Sophisticated management systems may be location- and network-aware — for example, only applying large software updates over low-cost high-speed networks such as Wi-Fi. Some device management systems also collect data from things to store in the cloud. The IoT also brings new problems of scale to the management task. Tools must be capable of managing and monitoring thousands and perhaps even millions of devices. The precise management needs will vary depending on the types of "things." Devices connected by cellular networks will often use a platform provided by the cellular network operator for monitoring and control functions related to cellular operations, and some of these platforms provide additional management functions such as firmware updates.

When? Management of complex IoT devices built using high-level operating systems such as Android is relatively straightforward because it can exploit platforms derived from related tasks such as mobile device management (MDM). Relatively mature platforms also exist in a few vertical areas; for example, BlackBerry provides an IoT platform for the automotive industry that includes a wide range of secure management functions integrated with QNX. However, secure management of very large numbers of simple "things" is much less mature, as are tools such as IoT platforms that may provide some device management features.

Who will be impacted? Any organization delivering large numbers of nontrivial connected "things" that need any form of postdeployment control or management.

Cautions: Many management platforms will be tactical decisions, so it may be necessary to change platforms during the life of long-lived things. Vendors selling tools derived from MDM are inexperienced in IoT and may not provide appropriate features or pricing models, and they may be subject to disruption as the mobile management market will consolidate significantly. The use of specific platforms mandated by the operator may be required for cellular-connected things.

Low-Power, Short-Range IoT Networks

What is it, and why is it important? Selecting a wireless network for an IoT device involves balancing many conflicting requirements, such as range, battery life, bandwidth, density (number of connected devices in an area), endpoint cost and operational cost. One important cluster of IoT networking technologies is focused on short range (tens to hundreds of meters), long battery life (years), relatively low bandwidth, low endpoint cost and medium density (hundreds of adjacent devices). For example, such networks will be essential in the smart home and smart office. Topologies include point-to-point, star and mesh networks (see Note 3). Some networks extend beyond basic communications to implement higher levels of the IoT stack, such as authentication and security. Network selection depends not only on technical factors but also on commercial issues such as what types of devices the network must talk to; for example, because few mobile phones support it, ZigBee is unsuitable for "things" that must talk directly to a smartphone.

In terms of unit shipments, low-power, short-range networks will dominate wireless IoT connectivity through 2025, far outnumbering connections using wide-area IoT networks. However, the commercial and technical trade-offs discussed earlier mean that many solutions will coexist, with no single dominant winner and clusters emerging around certain technologies, applications and vendor ecosystems. Current technologies include ZigBee, Bluetooth, Zwave/G.9959, Thread, Ant and Wi-Fi plus point-to-point systems on a range of industrial, scientific and medical (ISM) bands. More specialized technologies include examples such as EnOcean, which is used to implement battery-free remote switches by using energy harvested from the action of pressing the switch.

When? More than 10 technologies of this type exist today, and new technologies and variants of existing ones will emerge over the next five years. Examples of technologies likely to gain traction in the future include mesh Bluetooth, which could be important in the smart home, and Thread, which is sponsored by Google. Academic researchers are also working on novel ultra-low-power solutions based on ideas such as modulating ambient signals from nearby sources such as Wi-Fi.

Who will be impacted? Any organization designing wireless "things" for home, office or personal use.

Cautions: Because no technology or ecosystem will win the battle for the smart home or office, many environments will likely require gateways to convert between wireless protocols and devices.

The IoT implies many more objects using wireless, which could create noise and interference issues, so network designers must consider the impact of new wireless things on existing services such as Wi-Fi.

IoT Processors

What is it, and why is it important? The processors and architectures used by IoT devices define many of their capabilities, such as whether they are capable of strong security and encryption, power consumption, whether they are sophisticated enough to support an operating system, updatable firmware, and embedded device management agents. As with all hardware design, there are complex trade-offs between features, hardware cost, software cost, software upgradability and so on. In the IoT space, the choice of processors is often driven by which hardware and software is easily available to innovators, hence devices such as Arduino and Raspberry Pi have spawned many new products because the hardware and software tools were widely available at a very low cost to makers and experimenters.

Gartner predicts that low-end, 8-bit microcontrollers will dominate the IoT through 2019, which implies that many IoT devices will be extremely simple and incapable of running an operating system or performing sophisticated functions such as encryption unless built in as a hardware feature of the chip. Shipments of 32-bit microcontrollers will overtake the 8-bit devices by 2020; 16-bit processors will never become dominant.

Most enterprises won't design their own hardware devices, but will purchase them from external sources or commission specialist hardware designers to create them. However, system architects and security specialists must understand enough about IoT hardware to specify technologies that will satisfy their current and future business goals.

When? A very wide range of IoT processors is already available. Through 2020, the IoT will slowly become smarter as the use of 32-bit devices grows, enabling things to become more sophisticated and manageable.

Who will be impacted? System architects and staff responsible for security must understand what processor choices mean in terms of features, upgradability, cost and security.

Cautions: Understanding the implications of processor choices demands fairly deep technical skills. The IoT processor market is also a battleground where companies such as Intel are trying to displace established architectures such as ARM.

IoT Operating Systems

What is it, and why is it important? Traditional operating systems (OSs) such as Windows and iOS were not designed for IoT applications. They consume too much power, need fast processors, and in some cases, lack features such as guaranteed real-time response. They also have too large a memory footprint for small devices and may not support the chips that IoT developers use. Even platforms like Android, which has emerged from the mobile phone domain (which is a type of IoT application), are too complex and power-hungry for many embedded systems. Consequently, a wide range of IoT-specific operating systems have been developed to suit many different hardware footprints and feature needs. Several examples are illustrated in Table 1.

Table 1. Selected IoT Operating Systems

Examples of IoT Operating Systems	Approximate Memory Footprint
None — device uses bare hardware or some form of support library	None
Minimal embedded OS — e.g., Contiki, TinyOS, RIOT, Yottos	5KB to 50KB
Small footprint embedded OS — e.g., VxWorks, cut-down Linux	750KB to 1MB
Google Brillo	16MB
Full Linux with GUI, Android	0.5GB to 1GB

Source: Gartner (January 2016)

The minimal embedded IoT OSs are often very different from traditional platforms; many have event-driven programming models and some don't support modern high-level programming languages and features like multithreading and dynamic memory allocation. More modern minimal OS platforms such as Yottos and RIOT attempt to provide a more programmer-friendly environment without excessively compromising power consumption and memory footprint. In less constrained IoT devices with around 1 gigabyte (GB) of memory, IoT operating systems become more like conventional OSs, although they may still lack some features such as a sophisticated GUI. Organizations creating embedded IoT software will need to master the operating systems, programming models and development tools for small-footprint devices. Designers must understand the business trade-offs implied by OS selection; for example, a simple OS might imply less expensive hardware but more complex software development and could limit future upgradability.

When? A wide range of IoT operating systems is available. New embedded OS platforms are likely to emerge over the next five years, often from academic and open-source backgrounds.

Who will be impacted? Staff responsible for selecting, designing or developing embedded IoT applications.

Cautions: Embedded OS systems created by open-source projects are still relatively niche technologies, and skills and support may be scarce.

Low-Power Wide-Area Networks

What is it, and why is it important? Traditional cellular networks don't deliver a good combination of technical features and operational cost for those IoT applications that need wide-area coverage combined with relatively low bandwidth, good battery life, low hardware and operating cost, and high connection density. The long-term goal of a wide-area IoT network is to deliver data rates from hundreds of bits per second (bps) to tens of kilobits per second (kbps) with nationwide coverage, a battery life of around 10 years, endpoint hardware cost of around $5, and support for hundreds of thousands of devices connected to a base station or its equivalent. Such technologies are sometimes known as low-power wide-area (LPWA) networks or LPWANs.

A range of LPWA networking technologies have emerged to satisfy some of these needs; examples include Sigfox, Ingenu Random Phase Multiple Access (RPMA), LoRa, Long Term Evolution for machine-type communications (LTE-M), and more recently, a new cellular IoT standard, NarrowBand IoT (NB-IoT). A new variant of Wi-Fi — 802.11ah — operating at below 1 gigahertz (GHz) offers a range of around 1 km and may be suitable for some types of wide-area IoT applications. Some of these technologies can be deployed as private IoT networks; others are run by carriers.

When? Proprietary technologies such as LoRa, Sigfox and Ingenu RPMA are available now, and 802.11ah equipment will likely become available in 2016. Cellular IoT trials are being conducted with prestandard solutions, although standards likely won't be locked down until mid-2016, and widely available, proven endpoint hardware isn't likely until 2017 to 2018.

Who will be impacted? Any organization deploying low-bandwidth IoT devices over wide areas should explore LPWA networks. Example applications include smart cities, utility meters, environmental monitoring, equipment tracking and telemetry.

Cautions: The available technologies vary by country and sometimes even by city. There is as yet no established global standard with roaming support. Even when cellular IoT standards mature, the wide range of frequencies used by cellular networks may make international roaming difficult. Many LPWAs are proprietary, and some operate in unmanaged public spectrum, so they can't guarantee quality of service. The long-term commercial success of the proprietary technologies is uncertain. Cellular IoT is likely to dominate in the long term, but it is not yet available, which makes strategic choices challenging. Many of these technologies haven't achieved sufficient economies of scale to deliver on the promise of very low costs. Organizations developing long-lived "things" may need to make tactical networking decisions and modularize their hardware so that it can be replaced when better technologies are available.

Event Stream Processing

What is it, and why is it important? Some IoT applications will generate extremely high data rates that must be analyzed in real time (see the IoT Analytics section). Systems creating tens of thousands of events per second are common, and millions of events per second can occur in some telecom and telemetry situations. Traditional IT architectures that store and subsequently process data don't have the necessary performance to deliver real-time analysis of such data streams, and in any case, there may be too much data to store in its raw form. To address such requirements, distributed stream computing platforms (DSCPs) have emerged. They typically use parallel architectures to process very high-rate data streams to perform tasks such as real-time analytics and pattern identification. Examples include Apache Storm, Apache Spark, Google Cloud Dataflow and IBM InfoSphere Streams.

When? Several platforms are available now, although all are immature.

Who will be impacted? This will impact any organization whose IoT applications create extremely high-rate data streams that must be processed in real time — for example, telecommunications or oil industry telemetry.

Cautions: DSCPs are a new and immature product category. No vendor meets all needs, there are few standards, and applications cannot easily be ported from one system to another. Skilled developers are scarce.

IoT Platforms

What is it, and why is it important? IoT platforms bundle many of the infrastructure components of an IoT system into a single product. The services provided by such platforms fall into three main categories: low-level device control and operations such as communications, device monitoring and management, security, firmware updates; IoT data acquisition, transformation and management (for example, polling devices and storing data in the cloud); and IoT application development, including event-driven logic, application programming, visualization, analytics and adapters to connect to enterprise systems from vendors such as SAP. There are many such platforms (although not all of them provide all of these features). Example vendors include CubeNube, PTC, Eurotech, GE, Bosch Software Innovations and Axiros.

When? Many IoT platforms are currently available from a wide range of vendors, including startups and established companies. The market will be very volatile for several years because new entrants will continue to emerge and established companies will buy up products to build broader IoT product portfolios.

Who will be impacted? Organizations developing complex IoT systems should consider such platforms to jump-start projects because they deliver a wide range of necessary features.

Cautions: This is a very immature market and considerable technical and commercial volatility is to be expected. All such products are very proprietary, and migration from one to another is not simple. Many IoT platforms are expensive, with significant upfront license fees plus costs of up to a few dollars per "thing" per month, so they are unlikely to be viable for applications involving low-cost things or where things don't generate a recurring revenue stream.

IoT Standards and Ecosystems

What is it, and why is it important? Although ecosystems and standards aren't precisely technologies, most eventually materialize as APIs called by IoT systems. Standards and their associated APIs will be essential because IoT devices will need to interoperate and communicate, and many IoT business models will rely on sharing data between multiple devices and organizations. For example, the electric company might offer you a better price for power if their smart meter is allowed to control your washing machine. Many IoT ecosystems will emerge, and commercial and technical battles between these ecosystems will dominate areas such as the smart home, the smart city and healthcare. Many different types of IoT standards and ecosystems already exist. At the lower levels of the IoT stack, examples include communications protocols such as MQ Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), Data

Distribution Service (DDS) and Constrained Application Protocol (CoAP). As we move up the stack, APIs and ecosystems such as Apple's Homekit and Google's Nest will compete to own the smart home. Other examples of standards groups and alliances include the AllSeen Alliance, the OpenFog Consortium, the Thread Group, and the Open Interconnect Consortium.

There are too many IoT "standards," and in many cases, the concerns and technologies of these groups overlap or compete. Some groups have specific agendas, such as promoting their favored technologies or architectures. Many vendors hedge their bets by joining multiple groups, so their commitments to specific standards are rather tactical. There are also areas of IoT where standards are immature or incomplete, for example IoT security.

When? In 2016, there are many IoT standards and alliances; many overlap, most are immature, and in areas where there is considerable commercial potential such as the smart home, it's likely that the battles between standards and ecosystems will persist for three to five years. New standards will likely emerge in areas such as IoT security.

Who will be impacted? This will impact any organization designing or developing IoT solutions, especially job roles such as CISOs and architects who are likely to be selecting standards.

Cautions: Organizations creating products may have to develop variants to support multiple standards or ecosystems and be prepared to update products during their life span as the standards evolve and new standards and related APIs emerge. In some domains, such as the smart home, it's likely that converters and adapters will be required to bridge between competing ecosystems and protocols.

Additional research contribution and review was provided by: Leif-Olof Wallin, Ian Keene, Earl Perkins, Timothy Zimmerman, Dionisio Zumerle and Mike Gotta.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Secure Embedded Software and Systems in the Internet of Things"

"Three Best Practices for Internet of Things Analytics"

"Market Guide for IoT Platforms"

"Move to New Technology for Analytics on Fast Big Data"

"Cool Vendors in the Internet of Things 2015"

"Hype Cycle for the Internet of Things, 2015"

"How to Manage All Your IoT Endpoints"

Evidence

Information sources used in creating this research include Gartner market forecasts; discussions with clients, vendors and colleagues; academic papers; and reviews of crowdsourcing sites such as Kickstarter.

Note 1 Examples of IoT Security Issues

Recent examples of IoT-related security flaws in 2015:

- Hackers demonstrated their ability to take control of a Jeep remotely, killing the engine and disabling the brakes.
- A Wi-Fi-enabled kettle was shown to store unencrypted network security keys that could be extracted by hackers.
- A wearable fitness band was infected by malware that was then able to infect the smartphone, which was used to unload data from the band.
- Man-in-the-middle attacks were demonstrated on industrial control systems such as those used in power plants.
- Smart TVs were discovered to be transmitting audio and video information to a third party even when they were supposedly powered off.

Note 2 New Approaches to IoT Security

One example of one new approach to IoT security is physically unclonable functions (PUFs). These are functions whose response is based on physical properties of the electronics and varies between chips. So a PUF can be used to provide a hard-to-counterfeit response to challenges to authenticate an object.

Note 3 Mesh Networks

Mesh networks are ad hoc networks formed by dynamic meshes of peer nodes. Routing and control is distributed, and messages typically use a multihop strategy, jumping between nodes to reach their destination.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp