IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

Overcoming the Challenges of Enterprise IoT Adoption

February 2018

By Stacy Crook

Sponsored by Ruckus Networks, an ARRIS company

Introduction

The Internet of Things (IoT) is a natural evolution of the current technological and cultural environments. It will impact almost every industry and country around the world. IDC tracks IoT spending by organizations, governments, and consumers on a biannual basis and finds that the market momentum has been sustained year over year as stakeholders continue to invest in connected products and solutions. IDC predicts the worldwide IoT market spend will grow to $1.1 trillion in 2021, with a compound annual growth rate (CAGR) of 14.4%. The installed base of IoT endpoints will reach over 36 billion units by the end of 2021.

IDC defines the IoT as a network of uniquely identifiable endpoints (or "things") that autonomously connect bidirectionally. The IoT ecosystem contains a complex mix of technologies and services, including modules/devices, connectivity, IoT platforms, storage, servers, security, analytics, applications, and IT services. The creation of an IoT solution generally requires consideration of each of these elements. In addition, many organizations will need to determine if their existing IT architecture can support new IoT use cases.

Because of the complex mix of technologies required to build an IoT solution, there are several considerations for organizations. While many IoT deployments are driven by the line-of-business decision maker, it's critical that the IT organization be represented in the decision-making process because it will be involved in the management and maintenance of the solution over the longer term.

This Technology Spotlight highlights some of the opportunities and challenges that organizations may encounter in their journey to implementing an IoT solution. It also provides prescriptive considerations for making IoT technology decisions. A discussion of specific vertical applications — hospitality, education, and smart cities — highlights the need to make informed decisions about IoT technology investments.

As the IoT sees data being generated in industrial scenarios, it becomes increasingly important to have IT and operational technology (OT) on the same page so that the data is accessible to designated decision makers in a fast, reliable, and secure manner.

The Opportunities and Challenges of Deploying an IoT Solution

For many organizations, the IoT will be a key enabler of digital transformation. Data collected from connected machines can be used to create efficiencies, enhance product designs, develop new business models and improve customer experiences. Before any of these opportunities can be realized, however, companies must determine which use cases will deliver the most return on investment and the technology and services required to support the desired outcomes.

As mentioned previously, an IoT solution consists of various technology components, including endpoints, connectivity, and software. Oftentimes, services are required to help an organization integrate these disparate technologies into a working solution. On the surface, this might not sound much different from any other IT project. However, what can make an IoT project more challenging than other common IT projects are the volume and heterogeneity of the endpoints and the fact that too many conflicting standards options hinder communication between endpoints and communication between endpoints and other applications.

In addition to wide area cellular, WiFi, and wired connectivity, there are numerous other access types that are ideal for specific IoT applications — especially for those in near-field use cases. Bluetooth Low Energy (BLE) is a good example in that it communicates with objects in a predetermined area or range — which is ideal in industries such as retail, education, and hospitality. While BLE consumes little power, it has a robust radio that can operate to 100 meters and offers real-time data transfer. Zigbee is another wireless access technology characterized by low power consumption and low data rates that are adequate for applications such as door locks, light switches, and even some traffic management systems.

Low-power wireless access networks (LPWANs) represent an emerging network category. There are two different flavors of this connectivity — one using licensed (carrier-owned) spectrum (e.g., NB-IoT, CAT-M) and the other using unlicensed spectrum (e.g., LoRa). At a high level, LPWAN connectivity offers low power consumption with the ability to deliver signal over longer distances, which makes it a good option for many smart city applications.

Unlike the typical enterprise architecture, which consists of (fairly) homogeneous endpoints that communicate directly with servers behind firewalls on-premises or in the cloud over standard TCP/IP communications protocols, the IoT includes many different endpoint types. These endpoints vary in their compute power, battery life, and support of communications protocols.

Because of these complexities, organizations embarking on an IoT project are faced with many technical considerations, including:

- **What type of endpoints do we need to support our solution?** An IoT endpoint can be just about any computing device that doesn't require human interaction to communicate with another machine, so the possibilities are almost endless. Organizations must consider the level of computing power they need for the task the device will carry out, the battery life required for the frequency of communication and network the device will communicate over, the cost of the device, and the availability of staff with the appropriate skill sets to build applications for those device types.
- **What kind of connectivity is appropriate for our deployment?** IDC's latest *Global IoT Decision Maker Survey* asked IoT decision makers about the type(s) of connectivity they were using in their IoT deployments. With a mix of responses across all possible access types (e.g., WiFi, cellular, satellite, Zigbee), IDC concluded that the connectivity layer is still a complicated element of an IoT project. When organizations are deciding about the type of connectivity to use in their solution, they should consider the following:
  - Does the endpoint reside in a predefined area, or does is it move around a wider area?
  - Does the endpoint require real-time connectivity?
  - Does the endpoint consume a lot of power? Is it in an always-on state, or does it wake only when it performs a specific function?
  - Does the endpoint require high bandwidth to send large amounts of data, or does it send data only intermittently?
- **How do we manage network complexity?** Each time organizations want to add a device that uses a particular communication protocol, such as WiFi, Zigbee, or BLE, they have to build a network to support the deployment. This is a costly and time-consuming effort.

- **How will we manage and secure those endpoints?** Once organizations determine the appropriate mix of endpoint devices and how they will connect those devices to the Internet, the next challenge is to manage and secure the deployment at scale. In fact, IDC's *Global IoT Decision Maker Survey* overwhelmingly pointed to security concerns as the biggest challenge holding back IoT projects. The tools used to manage these devices must support the network over which the device is connecting and the device operating system (OS), which can present a challenge given the numerous combinations of networks and OSs that can exist. Many IoT endpoints are simple computing devices with few security capabilities built into more sophisticated devices, so when these devices connect to the network, they can represent a point of vulnerability in the network.
- **How will we collect and manage the data generated by these endpoints?** The next piece in the puzzle concerns data. IoT devices generate data at volumes that many companies are not yet well equipped to deal with, so they must evaluate the capabilities of their existing infrastructure in the areas of high-scale data ingestion, storage, and analytics. A related challenge is figuring out where data will be collected and processed — at the edge or in the cloud, or both. Edge processing supports reduced latency for time-sensitive applications and can also cut down on data transmission and storage costs. Organizations must also determine how they will integrate IoT data with other key systems of record and engagement. For instance, in the hospitality industry, combining IoT data with existing customer data can significantly enhance the customer experience.

Aside from technology considerations, the most successful IoT projects will also be well thought out from people and process perspectives. In fact, bringing the right stakeholders from around the company into the discussion is fundamental to future proofing technology choices. You may be building an RFP based around one use case, but your colleagues may have other applications for the technology that will require additional features.

IDC research finds that while the line of business is most likely to fund IoT projects, IT is often involved in funding to some extent. From IDC's perspective, IT should be brought in as early as possible because this group is usually responsible for setting up and maintaining the infrastructure over the long term to support the application the line of business wants to roll out.

In addition to the line of business and IT, other stakeholders may need to be involved. For instance, what are the legal implications of tracking a student around campus? Or, if you are trying to change your company's business model from a product-based orientation to a services-based orientation, might you need new skills within the organization to support that transformation? While the requirement to involve a representative from the legal or HR team in the IoT strategy team may not be obvious at first glance, these examples demonstrate the importance of thinking the project through from every angle.

Real-Life Applications of IoT

As mentioned, the IoT stands to have an impact in many vertical industries across the globe. In fact, IDC tracks spending in over 50 such use cases across 12 industry verticals on an ongoing basis. In the sections that follow, we explore how three industries can leverage IoT to improve operational efficiency, customer experience, and safety.

Hospitality

The IoT plays a key role in the digital transformation of the hospitality industry. Leveraging IoT, hotels will be able to improve everything from guest check-in to in-room experience to facilities management.

Instead of requiring guests to wait in a line to check in, hoteliers can provide mobile applications that connect with beacons for check-in and keyless entry. Once guests are inside the room, connected in-room devices provide the ability to monitor asset conditions, such as usage, temperature, and vibration, in real time. Companies can personalize the guest experience by linking IoT data with customer preferences.

For instance, when a repeat guest checks into his or her room, the temperature could be automatically set to his or her preferred temperature. When he or she turns the smart TV on, it could automatically tune to his or her favorite channel. When the guest gets hungry, dining recommendations could be offered based on past orders.

Expedited check-in and personalization of the guest room are two examples of how the hospitality industry can create a more engaging experience leveraging IoT data. Hoteliers can also utilize smart building technology to create more efficient environments — especially around HVAC and physical infrastructure such as elevators. These cost savings can ultimately result in additional funds to improve the physical aspects of the hotel experience as well.

Operating a hotel or a resort is an expensive undertaking. Building owners can deploy IoT technology that utilizes advanced automation and building systems integration to measure, monitor, control, and optimize operations. The goal is optimization — the deployment of a set of building systems capable of adapting in real time to both internal policies and external signals. These systems manage how building equipment operates to use energy in the most efficient and cost-effective way. The technology infrastructure of such an optimized smart building is defined by integrated control systems that automatically change settings and operational parameters.

Education

The educational experience can be redefined by IoT — inside and outside the classroom. Smart building technology can be utilized to create the optimal environment for student learning. Sensors can track environmental factors such as temperature, humidity, noise, and even carbon dioxide levels and attempt to link these factors to student focus.

Student safety is a key concern of most educational institutions; connected things can provide data on where students are throughout the school day. GPS-enabled school buses allow parents to track their child's journey to and from school each day. The introduction of IoT-enabled wristbands means that students can clock in and out of campus, ensuring their whereabouts are known throughout the school day. In addition, these wristbands can help ensure that intruders and other unauthorized people are not able to enter school premises.

College campuses can be spread out among multiple buildings in major cities and can be difficult for new students to navigate. The campuses can offer mobile applications that connect to beacons, which emit signals that give turn-by-turn directions to help visitors navigate their surroundings. These applications can not only ease anxiety but also help provide student security benefits.

Smart Cities

Cities all over the world are considering how the IoT can enhance the quality of life for inhabitants while saving costs. Public safety, smart parking, and smart lighting are three examples of applications for the IoT in cities.

Municipalities can leverage sensors mounted in high-crime areas to identify the sound of gunfire. In addition to identifying the sound of a gunshot, sensors determine the location of the gunshot, analyze the sound, and send data to connected police stations. The use of IoT can also give emergency crews quicker routes to a location by using highway sensors and adaptive traffic management. In addition, law enforcement agencies can use remote video cameras to better control evidence, speed response time, and lower crime.

Smart lighting optimizes lighting systems for commercial buildings to provide highly energy-efficient outcomes using sensors and software. Lights/ballasts are controlled/monitored remotely by building management system, application, business rules to controller, or other means. Integrating analyzed data (e.g., natural light cycles, room traffic, work schedules) allows lights to be tuned to meet specific objectives. Smart lighting then can be used as an operational resource for communication.

Smart parking refers to a sensor-equipped monitoring and reporting system that determines parking space availability through physical detection of vehicle presence (empty space or not). The system can include the integration of a payment system based on sensor value. Sensors come in different varieties — pressure, infrared, or thermal — and can be connected by a LAN to central management system software. Smart parking is attractive to cities because it can reduce congestion while increasing revenue.

Considering Ruckus as a Provider of Secure IoT Connectivity

Ruckus Networks, an ARRIS company, is a networking infrastructure vendor based in Sunnyvale, California. The company's portfolio of products and solutions aim to provide secure, reliable access to applications and services across any environment. This product portfolio includes access points, switches, and wireless LAN management and control, as well as a series of related SaaS applications that provide security/policy capabilities, network intelligence, and location.

Ruckus has traditionally focused on WiFi connectivity, one of the most popular methods of connectivity for IoT devices. WiFi has become a dominant connectivity method for IoT devices in both consumer settings, such as the home, and nonconsumer settings, such as buildings and campuses, because of its pervasive nature and applicability across a plethora of IoT use cases. However, as mentioned previously, each IoT use case has varying requirements; therefore, while WiFi can meet the needs of many applications, it is not the optimal connectivity method for all.

Challenges and Opportunities

As mentioned previously, the heterogeneous nature of IoT endpoints creates several complexities in IoT solution deployment. While the price of sensors has generally been driven down over the years, there is still a significant cost to build out the networks that support sensor communication. In addition to the initial buildout of the networks, organizations must consider the ongoing cost to manage, secure, and maintain the separate networks. Given the nascent state of the market, it is also wise to think about how this network will be able to accommodate new device types and communication protocols over time. These challenges are what led Ruckus to develop the Ruckus IoT Suite, a collection of network infrastructure components consisting of IoT-enabled access points; IoT modules for BLE, Zigbee, and LoRa; and an IoT controller to secure and manage the deployment. The IoT Suite integrates with the software that manages the existing WiFi infrastructure so that enterprises can bring new IoT device types into their environments without having to build out additional network infrastructure. In addition, this integration allows network administrators to onboard new devices as well as view, manage, and secure their entire wireless infrastructure through a single pane of glass. Ruckus has built a multitiered security architecture into the IoT Suite that protects data as it moves from the endpoint to the access point and on to its final destination.

IDC research finds that IoT budgets are on the rise, with 77% of respondents to a recent IDC demand-side survey stating that they had budget allocated for an IoT project in 2017 versus a mere 33% in 2016. Even though organizations are planning to spend more on IoT, there are still key concerns that delay projects. When participants in the same survey were asked to identify the top 3 challenges holding back IoT projects, 33.5% said security issues, 23.6% said up-front costs, and 22.2% said privacy concerns.

We can observe the applicability of these concerns in some of the use cases discussed previously in this paper. For instance, in an educational setting, devices that track students can provide peace of mind to parents that their children are where they should be. However, whenever the idea of tracking human movement comes up, privacy concerns are introduced. Hotels will also have to be very clear about what kind of information they are gathering about customers and allow guests to opt out of those programs if they desire. Cost is always an issue in nonprofit organizations such as public educational institutions and the state and local governments that fund smart city projects.

In IDC's research, potential security threats have stood out as the top IoT inhibitor year after year, and in these examples, it's clear that student, resident, and guest safety and security will always have to be a top priority.

As a provider of a solution that plays a role in network security, Ruckus has the opportunity to help customers understand how the IoT Suite can improve their overall IoT security posture. While it's true that deploying an IoT solution will often require some new investment, the ability to tie the new solution into existing WiFi administration tools can help cut down ongoing operational costs. Also, these tools can help manage device access, helping support privacy concerns.

Conclusion

The IoT is an immense opportunity that organizations around the globe will leverage to improve operations, create more engaging customer experiences, and transform business models. As we've discussed, there can be various opportunities to leverage IoT data even within a single vertical, such as improved guest experiences in the hospitality industry, student safety in the education vertical, and higher citizen satisfaction in the public sector. Organizations are eager to embark upon IoT projects; however, the trend is fraught with complexities spanning the endpoint, network/connectivity, and software layers, leading to concerns about security, privacy, and cost management. These concerns highlight the key role that IT must play in IoT deployments.

While we have pointed out that security remains a top inhibitor to IoT projects, it is also encouraging to note that IoT budgets are increasing year over year. In addition, an IDC survey found that over 55% of participants that had deployed IoT projects believe IoT increased their security posture, with 66% noting that their security posture had increased because the project prompted upgrades/improvements in IT security. Organizations that do not embrace IoT will be left out in the cold by organizations that do. Now is the time to imagine what can be done and figure out how to do it in the most secure, economical, and streamlined way possible.
