CHAPTER

APPLICATION MANAGEMENT IN THE INTERNET OF THINGS 15

The Moving Finger writes: and, having writ,
Moves on: nor all thy piety nor wit
Shall lure it back to cancel half a line,
Nor all thy tears wash out a word of it.
Rubaiyat 51, Rubaiyat of Omar Khayyam

Before proceeding, it is first necessary to address the question of "What is meant by the **Internet of Things (IoT)**?" There are conflicting views about a concrete definition. The situation is reminiscent of the Indian fable of "The Blind Men and the Elephant." In that fable, a group of blind men are asked to describe an elephant. Each man felt only one part of the elephant. This resulted in each man having a very different perception of what an elephant was like (a pillar, a rope, a tree branch, a hand fan, a wall, a solid pipe, etc.) (Fig. 15.1).

There is still a great deal of confusion about IoT, much of it due to the phenomenon characterized by the fable of "The Blind Men and the Elephant." It is still a work in progress, with work going on in countless, semi-isolated groups around the world. An explosion taking place in slow motion would be another analogy. It will be at least a few years until IoT begins to stabilize, if that ever happens. However, for the sake of this chapter, it is important to provide some definition of the space even if those definitions are superseded in coming years. For this book, we will rely on a definition developed by Enterprise Management Associates. "The Internet of Things (IoT) is an interconnected web of sensor-enabled devices that communicate between each other and a series of intermediary collection points. This web of devices provides sensor information on device operation, status, and location" (Fig. 15.2).[1]

IoT is a concept that has been around since at least the 1990s. However, it was not until the 21st century that the necessary technologies emerged and began to coalesce. The developments that were needed to take IoT from an academic pipe dream to reality include:

- Miniaturization of components
- Commoditization of components leading to substantially lower costs
- Concise, compact software (microcode)
- Ubiquitous connectivity

[1] "The Rise of the Internet of Things: Connecting Our World One Device at a Time." Myers and Wise, EMA, 2016.

Application Performance Management (APM) in the Digital Enterprise. http://dx.doi.org/10.1016/B978-0-12-804018-8.00015-2

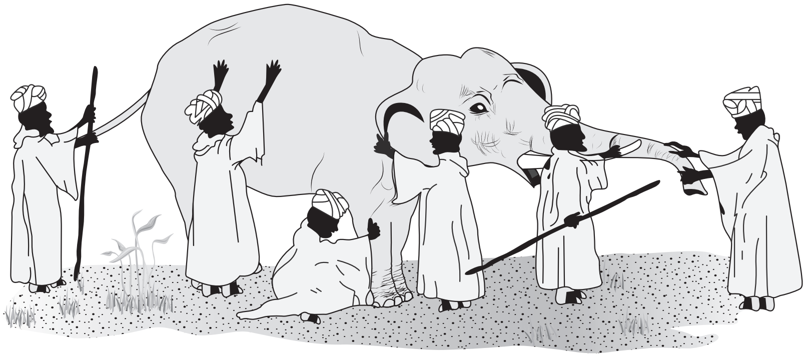
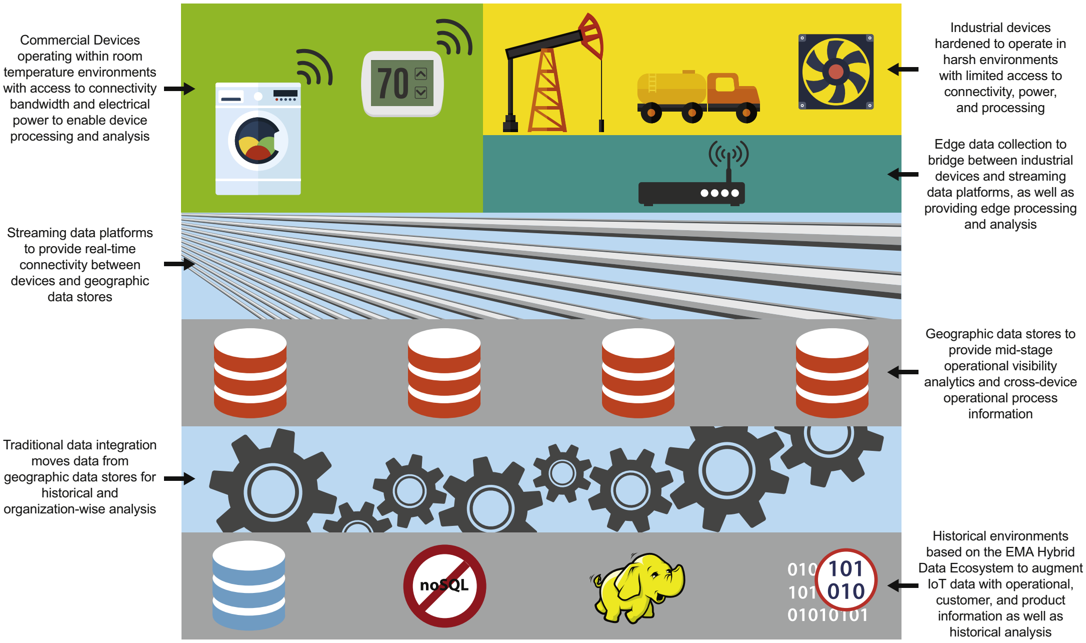


FIGURE 15.1

Blind men and the elephant.

> "The Internet of Things (IoT) is an interconnected web of sensor-enabled devices that communicate between each other and a series of intermediary collection points. This web of devices provides sensor information on device operation, status, and location."[2]



Commercial Devices operating within room temperature environments with access to connectivity bandwidth and electrical power to enable device processing and analysis

Industrial devices hardened to operate in harsh environments with limited access to connectivity, power, and processing

Edge data collection to bridge between industrial devices and streaming data platforms, as well as providing edge processing and analysis

Streaming data platforms to provide real-time connectivity between devices and geographic data stores

Geographic data stores to provide mid-stage operational visibility analytics and cross-device operational process information

Traditional data integration moves data from geographic data stores for historical and organization-wise analysis

Historical environments based on the EMA Hybrid Data Ecosystem to augment IoT data with operational, customer, and product information as well as historical analysis

FIGURE 15.2

IoT Ecosystem Reference Architecture.[3]

[2] Ibid.

[3] Ibid.

- Low overhead communications protocols
- Technology for processing vast amounts of data (i.e., Big Data and analytics)
- Methods for uniquely identifying devices

Every time a new technical innovation emerges, there is a period in which the market struggles to sort out the nature of the innovation, how it will be applied, and what terminology will be used to describe it. Concurrent with this is something like a cattle stampede, as vendors rush to try to capture a share of the new market, or at least leverage the excitement around it to stimulate sales of their existing product(s). Each company has its own marketing messages, each with a unique interpretation of what the new technology is or how it can be used, and/or how it impacts other current markets. While generally well intentioned, this multitude of perspectives does make it difficult to sort out the true nature of that innovation.

It is not possible to know how many objects are currently deployed with instrumentation for IoT purposes. Even the best attempts to estimate that number are little more than educated guesses. It is enough to know that there is a very large number (currently in the billions) of objects deployed and that number is likely to increase by orders of magnitude in the next few decades.

The market for IoT products can be divided between consumer and commercial and government applications. For consumers, IoT applications range from frivolous to life-saving. The following are some categories with a few examples. It is important to realize that these categories are only examples and that there are many others (Fig. 15.3).

FIGURE 15.3

IoT connecting everything to everything.

Health

Monitor vital signs (applications for all ages)
Ensure that medication is taken
Implanted devices
Track activity levels
Track location

Home

Security (smart access)
Home automation (smart appliances)
Energy efficiency (lighting, heating, and cooling)
Irrigation

Lifestyle

Toys
Drones
Wearables (smart watches, FitBit, etc.)
Smart cars (autopilot, preventative maintenance, etc.)

Below is a similar list for IoT applications in business and government sectors. Again, it is important to realize that this is just a list of examples and is not intended to be exhaustive. There are many other areas where IoT will be applied (e.g., mining, military, hospitality industry, etc.). The list of areas where IoT can be applied is virtually endless.

Smart cities

Traffic management
Parking management
Mass transit management
Area lighting
Crowd monitoring and management
Monitor water usage and waste water handling

Manufacturing

Preventive and predictive maintenance
Quality control
Flow management (smart valves)
Inventory control
Tracking
Information to support police and fire services
Employee safety

Retail

Inventory control
Loss prevention
Targeted marketing

Smart lighting
Track customer behavior
Adaptive pricing

Agriculture

Livestock monitoring (health and location)
Discrete application of fertilizer
On-demand irrigation
Monitor plant health
Inventory control (seed stocks, harvested crops, etc.)

Health

Ambulance telemetry
Hospital asset tracking
Access control
Implanted devices
Patient monitoring
Asset management

Energy

Smart grid (electrical distribution)
Flow management (pipelines)
Smart valves
Smart meters
Smart air conditioning controls (utility can turn off during peak demand periods)

Natural resources

Wildlife monitoring and tracking
Forest management (health and prevent illegal logging)
Wildfire crew tracking
Monitor human impacts

INSTRUMENTATION

The first point that must be understood about IoT is that it is not a "thing." It is not a tangible object that can be touched, weighed, or measured. It is not an intangible article such as software, nor is it a service to which one can subscribe. It is more accurate to think of IoT as a phenomenon. It consists of billions of objects around the world that are instrumented, and the instrumentation is generating unimaginable amounts of data. It is that instrumentation that is the enabling force behind IoT and it is the instrumentation that is central to IoT.

For IoT to work, there must be instrumentation with the following attributes:

- Power source(s)
- Memory
- Operating system and application software

- Data collection by the associated object
- Ability to communicate with a higher level system
- Control over the associated object (optional)

Those are the attributes of the instrumentation, but what is the instrumentation? That is, what form does the instrumentation take? In the simplest terms, the instrumentation required for an object to be part of IoT is a computer system. Most commonly, that computer system consists of some microcode running on a single chip or a board. However, in principle, code running on a **PC** or even a server could perform the same functions and in the case of large complex systems (e.g., manufacturing, traffic control, etc.), a larger system may be better suited.

Generally, the IoT remote system will reside within the object with which it is associated. However, it is possible for the IoT system to be external to its object. In either case, the IoT system must be attached to data sources. Those data sources may be sensors that were embedded to collect data for the IoT system. Alternatively, the IoT system may utilize data that is collected by the object for operational purposes. In the case of the latter, the IoT system must have a way to extract that operational data.

IMPLEMENTATION

Because of the magnitude of the IoT space, the diversity of uses, and the absence of widely accepted standards, a significant disparity in implementations is inevitable; therefore, it is inescapable that there will be many exceptions to the following description. Nonetheless, the definition presents the most common approach to implement IoT.

The software for an IoT component is written on **non-volatile memory (NVM)**. That is necessary so the code will be secure and remain intact if there is a loss of power. Being secure means that it is not possible for the code to be altered or reverse engineered. Likewise, any **encryption** keys that are used must be fully protected from discovery or alteration. It is important to remember that objects with IoT instrumentation will often be found in remote locations where there is little or no physical security. Also, the environmental conditions may be extreme. Any solution must be able to perform satisfactorily in such environments.

The use of **one-time programmable memory (OTP)** memory, including PROM and ROM, will typically achieve these objectives. The software is printed on a **complementary metal–oxide semiconductor (CMOS)**[4] chip, using standard manufacturing processes. Once printed, the information on the chip is relatively secure.

MANAGEMENT

Management of IoT applications poses some unique challenges, and in other ways is much simpler than traditional applications. There are two parts to IoT applications: the portion that runs on and monitors a remote object and the software that resides upstream from the remote software.

The upstream applications are the ones that collect data from the remote applications. They reside on a much more robust system (whether it is a PC, server, or mainframe of something else is irrelevant). At a minimum, the upstream applications collect data from the remote applications and store that data

[4] CMOS is a technology for constructing integrated circuits (chips). It offers the advantages of low power consumption and low waste heat. Both traits are important in IoT components. CMOS is the dominant form of integrated circuit manufacturing.

in some kind of repository. That repository may be proximate to the application or situated remotely. That is, the remote repository for data at rest may be on the same chip as the remote application, or it may be stored elsewhere on the remote device.

Each of the upstream applications is in every sense an application and the management of them is the same as it is for any other application, regardless of the environment where they run (e.g., local server, PC, mainframe, cloud-based systems, etc.). The same management functions (fault, performance, accounting, and security) are required and the same tools can be used as would be used for any other applications running in the same operating environment (i.e., with the same operating system).

CONFIGURATION

The situation is very different with the remote applications. In simplest terms, the application can be viewed as installed and configured at the time of the manufacture of the chip set on which it resides and runs. If the designer elected to use NVM OTP CMOS technologies for the implementation, then like the quote at the beginning of this chapter, it is finished. It would seem that there is no practical way to change what was written. However, there does need to be a way to capture user preferences, local access codes, etc. Also, in order to avoid having to replace an entire IoT remote system, the designer may elect to allow patches or new copies of the code to be written to the chip. Currently, there are multiple techniques available for accomplishing this and new ones are likely to emerge in the future. While a thorough discussion of the technical details of how this can be done is beyond the scope of this book, it is important to note that if changes are allowed, the security of that application is weakened.

A designer can select a variety of chip options, including **programmable read-only memory (PROM)**, **field programmable read-only memory (FPROM)**, **erasable programmable read-only memory (EPROM)**, and others. Any of these may be chosen for special IoT applications to meet the individual architectural and use requirements of the intended IoT applications, but each also has limitations and/or special requirements (power and/or UV light) that limit their usefulness in certain environments or use cases, thus affecting it for widespread use for IoT. Also, use of one of these alternatives can compromise the integrity of the software due to environmental factors or external threats.

SECURITY

One may be tempted to question the importance of the need for security for IoT applications – especially when thinking about consumer-focused applications such as the smart home (e.g., lighting, smart thermostats, smart appliances, etc.) or some wearables. However, there are many more important uses for IoT applications such as traffic control, mass transit (i.e., trains and subways), oil refineries, utilities, factories, hospitals, etc. with the potential for catastrophic consequences from an error caused by a cyber attack. We live in a world where acts of terror are commonplace, where some people find enjoyment in simply proving that they are able to hack into a system regardless of the consequences, and where state-sponsored cyber attacks are rampant. Thus far, the latter have been relatively benign, possibly intended only to ensure that the capabilities exist if there is ever a need to call on them. However, state-sponsored attacks have potential to wreak havoc throughout a country. Even if IoT is more passive (i.e., just collecting data and forwarding it to an upstream system), it is important to ensure that the application and its data are secure. That is because that data can form the basis for future actions and some with potentially serious or even deadly consequences if the wrong action is taken.

The use of NVM OTP CMOS technologies enables relatively tight security for the application. Together, these technologies can make it difficult or (depending on the design) even impossible to alter the software on the chip(s). The data that is captured by the remote application and stored remotely must also be protected. It is vulnerable unless it is encrypted. Therefore, encryption for both the data stored on the IoT remote system (data at rest) and data in transit is necessary. Even when stored data is encrypted, it may be possible to delete data and thus cause harm. In all honesty, for most cases, this is a relatively esoteric discussion. Destruction of data requires an attacker to have physical access to remote IoT systems, or to have compromised the encryption used for communication with the upstream application(s) and any additional security measures that were implemented. Certainly, it is possible to do that. However, to do so requires the dedication of a tremendous amount of resources (or the assistance of an insider). Attacks involving the assistance of an insider are much more difficult to prevent. Some would say, depending on the role of the insider, it is nearly impossible to prevent successful insider attacks (Fig. 15.4).

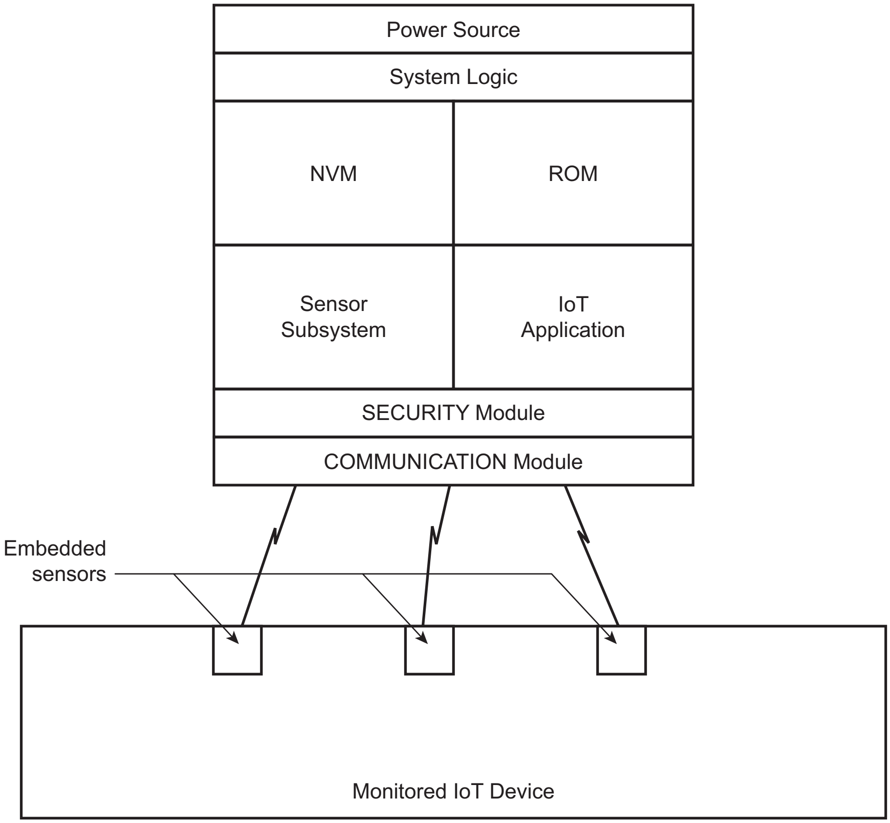


FIGURE 15.4

Simplified view of remote IoT device.

As mentioned earlier, data in transit encryption is a crucial consideration for the security of the collected data to be maintained. This form of encryption prevents “man in the middle” attacks. However, data in transit encryption is only part of the strategy. Next, the network itself must be secured with latest techniques available. However, at a minimum, the network needs to utilize IPsec, SSL, SSH, WPA, etc. or an equivalent technology to encrypt each packet and to authenticate each node in the communication stream. The use of other **virtual private network (VPN)** capabilities may also be warranted along with security these measures.

FAULT

Limited monitoring is possible with an IoT remote application, but only if the application was designed to support management queries. While it is possible to incorporate a management agent, the design objective of minimum use of memory conflicts with this. Instead, awareness of the health of the remote application and system (i.e., chip set) on which it runs is largely a function of interpreting the data supplied by the remote application, recognizing when it is no longer communicating, and understanding that the data it is communicating outside of the expected range. In that event, it may be possible to remotely interact with the system to run some form of testing or power cycle the system on which the IoT remote application resides. If that fails to resolve the problem or if the system does not support remote power cycling, then it is necessary to dispatch someone to replace the failed system. At this point, it is important to remember that most IoT systems (units) are inexpensive to the point of being disposable.

PERFORMANCE

The overall performance of the remote application is equivalent to end-to-end response time in real-time systems. It is a composite of the performance of sensors, the remote application, and the network over which the data from the remote application is transported. Obviously, network performance is something that can be managed and fine-tuned, and that is routinely done. The performance of the remote application is determined at the design and testing stage. In general, once the application is burned on the chip, its performance is permanently defined. The exception to this is if there are user-defined parameters that can impact the performance of the application. If there are, then those can be adjusted with their overall performance increased or decreased accordingly. Hopefully those adjustments to user parameters can be changed remotely, otherwise someone will have to travel to the location of the remote application to make the change. Unless the remote application was specifically designed to capture and report certain metrics about its performance, it will not be possible to capture that information.

ACCOUNTING

As explained in Chapter 3, the accounting component of **application management** of applications consists of two basic functions: asset management and tracking of resource utilization. In fact, such information would most likely be of limited value given the relatively static nature of the remote application. The system on which the remote application runs is a closed environment. The remote application can only use resources that are part of that system (with the possible exception of power).

The other aspect of accounting is asset management, which is definitely relevant to the management of IoT remote applications. Each system should have a unique identifier. It may be a MAC address, a serial number assigned to the chip on which the remote application runs, or a custom identifier developed by the designer (or the designer's employer). Through this unique identifier, it is possible to individually account for each IoT system. That identifier can also be tied to the IP address for each system to more granularly identify the system and has an additional benefit of enabling additional security features in some designs.

In 2015, researchers discovered that makers of a wide assortment of embedded devices were reusing HTTPS certificates and SSH keys. In doing so, they were potentially defeating the very security that was supposed to be enabled by those certificates and keys.

Passive Identifiers

Passive, permanent identifiers such as barcodes, **quick response codes (QR codes)**, and **radio frequency identification (RFID)** tags are *not* part of the Internet of Things. It is true that they represent data that can be collected, but that data is static. It is fixed at the time of manufacture of that object or when the label or tag is attached. They are actually quite similar to a brand (or ear tag) on a cow or a retina pattern in a person's eye. Each is unique and can be read. They certainly contribute to the exponential increase in the volume of data being captured and stored. However, they lack the data collection and communication attributes required for them to be part of IoT.

The devices that read the passive identifiers are sensors in the IoT hierarchy. Those devices are likely to also include the remote applications necessary to communicate the data collected with an upstream application. The passive identifiers represent data points that are detected by a sensor, just as a sensor might detect engine temperature or atmospheric pressure.

SUMMARY

The Internet of Things (IoT) is a technology experiencing explosive growth. It holds the promise to revolutionize how we live and work. Successful realization of the potential of IoT requires the effective management of the applications that make it possible. Management of applications that are physically attached to the objects that they collect data from (i.e., remote applications) requires special attention at the design/test stage and once they are deployed and operational.

Upstream applications (i.e., the ones that receive data from remote applications) do not require any special management consideration. They can be managed like any other application running in the same environment (mainframe, server, PC, etc.).

KEY TAKEAWAYS

- There are billions of IoT objects currently deployed and the number will continue to grow dramatically.
- IoT devices will have a dramatic impact on how people live and work. Because of that, it is imperative that the IoT applications be well designed and manageable.

- Management of host-based (mainframe, server, PC, etc.) applications is comparable to the management of any other application in the same environment.
- Remote applications will usually reside on a single CMOS chip.
- Applications that are printed to a chip using OTP NVM CMOS are difficult to modify. Thus, management is more difficult.
- Greater care must be taken when designing and testing applications that will be installed on remote objects.
- Since IoT devices are often remote and unattended, greater attention must be given to designing the system to be secure.