Brought to you by:

arm

IoT Solutions

for dummies

A Wiley Brand

Design a robust, scalable IoT solution

Manage deployment

Stay secure and connected

Lawrence C. Miller

2nd Arm Special Edition

About Arm

Arm defines the pervasive computing that shapes today's connected world. Realized in 110 billion silicon chips, Arm's device architectures orchestrate the performance of the technology transforming our lives — from smartphones to supercomputers, from medical instruments to agricultural sensors, and from base stations to servers. Every day thousands of Arm partners embed more than 45 million Arm-based chips in products that connect people and enhance the human experience, to serve today and architect tomorrow.

Arm's Pelion IoT Platform is a flexible, secure, and efficient foundation spanning connectivity, device, and data management. It accelerates the time to value of IoT deployments by helping partners easily connect trusted IoT devices on global networks, invisibly administer them, and extract real-time data from them to drive competitive advantage.

To discover more, please visit **Arm.com/pelion**.

IoT Solutions

2nd Arm Special Edition

by Lawrence C. Miller

for dummies®
A Wiley Brand

IoT Solutions For Dummies®, 2nd Arm Special Edition

Published by

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

www.wiley.com

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-65675-3 (pbk); ISBN 978-1-119-65676-0 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner

Senior Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Magesh Elangovan

Introduction

The Internet of Things (IoT) is creating a global network of connected and intelligent devices that will inform and enhance society and business. Many important challenges and design considerations, such as regulatory requirements and post-deployment management of IoT devices, must be addressed early to build a complete, scalable, and secure IoT solution.

About This Book

In this book, you'll learn what is required to design a robust and scalable IoT solution serving a range of markets and needs, including important challenges to consider and why it is vital to address those challenges at the earliest stages of planning and design.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless! I assume you work for a company that is interested in building an IoT solution to support the delivery of data-driven services for your customers, or for optimizing your own processes and assets. Perhaps you're a CIO or the director of an engineering team responsible for key decisions related to the planning and design of your IoT

solution. As such, I assume some technical knowledge and familiarity with IoT enabling technologies. If any of these assumptions describe you, then this book is for you!

Icons Used in This Book

Throughout this book, I occasionally use icons to call out important information. Here's what to expect.

This icon points out information you should commit to your nonvolatile memory.

You won't find a map of the human genome here, but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon.

Tips are always appreciated, never expected. I hope you'll appreciate these useful nuggets of information.

This icon points out the stuff your mother warned you about (well, probably not). But these helpful alerts do offer practical advice.

Beyond the Book

There's only so much I can cover in this short book, so if you want to learn more, just go to `www.arm.com/pelion`.

IN THIS CHAPTER

- Explaining the Internet of Things
- Leveraging a complete IoT ecosystem

Chapter 1
The IoT's Business Implications

In this chapter, you learn about the Internet of Things (IoT): what it is, what opportunities and challenges it presents, and why a complete innovation ecosystem is critical for success.

Defining the IoT

The IoT is a network of *physical* objects (such as wearable devices, home appliances, security systems, personal and commercial vehicles, nanotechnology, manufacturing

equipment, and more) embedded with *smart* components (such as microprocessors, data storage, software, sensors, actuators, and more) and *connected* to other devices and systems over the Internet.

At the micro scale, the "thing" may be an individual component, such as a smart lighting unit in a commercial office building, or the building itself, as an item in a portfolio of assets being tracked.

The value of the IoT is in the data that is collected and then analyzed to provide insights or actions. To ensure the integrity of that data, the whole system must be secure and managed.

A vital part of that is the choice of connectivity protocol. System sustainability depends upon being able to reliably transmit different types of data over a variety of distances and through a broad array of materials in the most energy-efficient way possible. The efficiency element is critical because many IoT applications depend on battery-powered sensors, whether that sensor embedded is in an electric vehicle or buried in a farmer's crops.

IoT devices may collect, store, and share data and/or perform advanced control functions — such as smart meters and light bulbs, autonomous vehicles, and sophisticated industrial equipment — increasingly using artificial intelligence (AI) and machine learning (ML).

Looking at the IoT's Rise

A recent Economist Intelligence Unit (EIU) IoT Business Index surveyed executives and senior business leaders from around the world. Fifty percent reported that IoT was an important part of their business strategy and that many of those companies were already rolling out IoT services.

By 2022, the combined Industrial Internet of Things (IIoT) market in North America and Europe is expected to be worth more than $1.2 trillion, with a compound annual growth rate (CAGR) through 2021 of 13.1 percent and 11.9 percent, respectively, according to Mind Commerce.

Avoiding Potential Pitfalls

As with any rapidly evolving opportunity, significant challenges must be addressed in the IoT market. Perhaps the biggest pitfall to avoid is failing to define a commercially viable business model. You need to clearly define the use case and capture the business requirements for the problem being addressed — for example, providing a service, product lifecycle engineering, customer satisfaction, or operational efficiency improvement — and align all your efforts toward solving that problem.

WARNING

An IoT system designed without the customer at the center is frequently doomed to fail.

Another common pitfall for an organization is failing to adequately navigate the digital transformation an organization must go through if it is to capture the benefits of IoT, especially at scale. It is important to have a plan across divisions and/or functional groups. Pitfalls to be addressed include:

- **Scalability and efficiency:** Building any network requires careful consideration and design flexibility to achieve scale. This ranges from the type of devices and network designs employed for particular use cases to the broader question of whether the industry has the right engineering resources to attack the problem (see Chapter 2).
- **Management and connectivity:** To scale IoT, hardware and software must be considered in tandem and implemented up front because the long-term resiliency and usefulness of an IoT solution must be constantly managed and optimized (see Chapter 3).
- **Security and social responsibility:** Cybercrime costs the global economy one-half trillion dollars a year in economic losses, ransom payments, and dealing with the resulting chaos. Although the advantages of what a connected world can do for people and businesses still vastly outweigh the threat, businesses must ensure that they can maintain trust in the system. To do this, business must act collectively and accept that all technology

companies share the responsibility to deliver collectively on the promise of secure devices and systems (see Chapter 4). A holistic set of threat models, best practice documentation, and open source reference firmware, commonly known as the *Platform Security Architecture* (PSA), can act as a good starting point for consistent application of security at the hardware and firmware levels.

Recognizing the Need for an IoT Ecosystem

The IoT market is characterized by the rapid development of new products, software, and technologies. In this fast-paced environment, industry standards and government regulations can be outdated, because they typically fall behind the breakneck speed of innovation for the world of tomorrow. Thus, technology vendors must be proactive in their efforts to ensure interoperability with other technology vendors in the IoT ecosystem, improving communications and transparency around cyberattacks and exploits, to ensure effective security.

REMEMBER

Scaling to billions of devices means that technology and people must work together. From cloud software to connected sensors, your IoT ecosystem must provide the solutions you need.

Examples of services and the value proposition in a robust partner ecosystem include design services, such as system on chip (SoC) design, software integration, and hardware customization, as well as these support services:

- **Training**
  - *Reduce risk* (equip engineers with required knowledge)
  - *Accelerate time-to-market* (start designing sooner and complete in a shorter time frame)
  - *Motivate the team* (improve confidence in design)
- **Design reviews**
  - *Reduce risk* (identify design issues while they can still be easily fixed)
  - *Ensure success* (avoid flaws that could limit the functionality of your product)
  - *Expert review* (get assistance at key stages throughout your design)
- **Technical support**
  - *Comprehensive, accessible documentation*
  - *Fast resolution* (expert assistance to resolve technical issues quickly)

IN THIS CHAPTER

- Starting with IoT platform requirements
- Evaluating design choices
- Looking at hardware

Chapter 2
Building a Scalable and Efficient IoT

In this chapter, you learn about the basic requirements for IoT devices, IoT deployment options and design choices, plus different IoT platform hardware approaches.

In the race to the "next big thing" for the Internet of Things (IoT), businesses must define their unique technical requirements. However, there are four crucial requirements for the IoT in general:

- **It needs to work separately.** The different components of an IoT solution must be able to

function independently, and be managed independently, as well as a part of the whole.

- **It needs to work together.** Otherwise, the return on investment (ROI) for connecting them in an IoT solution is reduced. They must communicate with each other and with the cloud to make the best and most efficient use of collected data.
- **It needs to leverage automation.** ML, as an enabler of AI, will play an increasingly important role in IoT devices. A case in point is image recognition, in which a system can be trained to determine, with a high degree of confidence, whether it's looking at different objects such as a child or a cat. Some image recognition is simple enough that it can easily be handled in the camera itself. This capability reduces latency and communications bandwidth while improving user privacy in some cases. ML is becoming more distributed with functionality available at the edge of the device network. This allows both learning and training at the edge, so devices have ML capability independent of the cloud. This improves latency and offers greater security.
- **It needs to work resiliently, securely, and safely.** Security requires heightened focus from the edge to the cloud to protect against both known and unknown threats. Part of this is to make end-users do much less of the work in the security chain, and make that work invisible for them as

part of their daily routines. Connected IoT devices must also work reliably and operate safely.

Exploring Your Options

The deployment of IoT devices at scale requires flexibility, coverage across a vast range of IoT client devices, and communications efficiency. With easy integration and increased developer productivity, enterprises can rapidly roll out and manage full-scale deployments. Traditional cloud-based device management services can simplify the provisioning, on-boarding, securing, and updating of devices across complex networks. Alternatively, on-premises or hybrid solutions offer greater control and security over devices and data.

Connecting the old

Business cases for IoT deployment differ depending on the level of "connectedness" already in a system, as well as the amount that will be required in the future.

Many companies already have some sort of tracking or sensor-based regime in place; in particular commercial buildings, goods transportation, and utilities. Yet their current technologies may not allow for individual tracking — that is, individual IP addresses for each sensor. Upgrading to a full-scale IoT system would provide a

major improvement in the value they can get from data, in terms of the quality and quantity of the data.

In this case, a way of linking from the existing device data network to a gateway that allows full remote management via the Internet is required. Systems with this capability are now readily available.

Connecting the new

Whether you are looking to connect an intermediary device to "passport" data from an old network to a new one, or are building a new system using advanced digital sensors (32-bit/64-bit) from the start, you need to consider how devices will be managed.

Today's increasingly complex IoT use cases strongly benefit from endpoint devices that leverage an embedded operating system (OS) that brings a comprehensive suite of security and connectivity elements.

Although having an OS is not mandatory, IoT devices are growing in complexity due to nodes having more sensors, data processing, and connectivity to send data. The use of an OS, in particular a real-time OS, simplifies the job of application programmers and system integrators because many low-level challenges are taken care of by the OS. Some important OS characteristics include:

- **Modular:** On-device libraries allow you to concentrate on writing application code.

- **Secure:** Including isolated security domains, secure over-the-air (OTA) updates, threat models, and Transport Layer Security (TLS).
- **Connected:** Support for a wide range of connectivity options with drivers for:
  - Ethernet and Wi-Fi
  - Cellular, including 3G, 4G Long-Term Evolution (LTE), LTE Advanced, LTE Advanced Pro, 5G (in development), and NarrowBand Internet of Things (NB-IoT)
  - Bluetooth classic and Bluetooth Low Energy (BLE)
  - Low-power alternatives, including Bluetooth Low Energy, Bluetooth mesh, IPv6 over Low power Wireless Personal Area Networks (6LoWPAN), Long Range (LoRa) LPWAN, Thread, ZigBee, and others
  - Near-field communication (NFC) and radio-frequency identification (RFID)

Considering Hardware

IoT use cases can be simple sensor devices existing for ten years or more on a coin cell battery and transmitting "tiny data" periodically over long distances (such as in a field or on an oil rig). They can be RFID "smart tags"

tracking goods on pallets. They can even be embedded building sensors that may be mains-powered.

The key in the vast majority of applications is energy efficiency. Important considerations include energy profile, MCU/CPU security (basic to strong), and connectivity protocol (distance, power, security).

Most IoT devices will not be mains-powered, so the main IoT chip must use a highly efficient architecture. This can be off-the-shelf or a custom system on chip (SoC) based on standard IP components.

Off-the-shelf requires a vast choice of products so that your design is scalable. Many IoT devices evolve as the value of collecting data increases and the product needs greater compute power. You need access to performance options and the ability to tie into other intellectual property (IP), such as digital signal processors (DSPs), to bring all your sensors together (sensor fusion).

Whether you choose off-the-shelf or custom SoC, either choice will require easy access to design tools, approved design houses if you don't have in-house expertise, an established and expansive software ecosystem (experienced in working with your chosen chip architecture), and foundry partners equipped with relevant performance optimization pack (POP) IP to manufacture your chip in the most effective way possible.

IN THIS CHAPTER

- Deploying device updates
- Rolling out security patches
- Scaling to thousands of devices
- Staying connected

Chapter 3
Managing IoT Deployments

In this chapter, you learn about updating devices in the field, patching security vulnerabilities, managing thousands of IoT devices at scale, addressing legacy and on-premises systems, and maintaining connectivity in diverse and challenging operating environments.

Updating Devices

One of the major challenges facing IoT deployment is addressing the operational needs of devices throughout

their lifecycle, particularly in ensuring that devices have the correct software installed, that firmware is protected against security vulnerabilities, and that application and functionality updates are managed.

IoT devices typically have a product lifetime of 10 or more years. Over the lifetime of a product, there is a need to unlock additional business potential, address functional defects, and manage constantly evolving security challenges. Remote over-the-air (OTA) software updates are the most efficient way to distribute and install required software changes.

Key requirements for updating IoT devices include:

- **Secure:** The authenticity and integrity of updates should be verifiable.
- **Fail-safe:** Update campaigns should be protected during power failures.
- **Campaign tracking:** Accurate campaign tracking reduces maintenance costs.
- **Succinct:** Delta updates administer specific elements of an update rather than an entire update campaign to minimize energy consumption.
- **Conditional control:** Business rules should prevent interruption of critical device operations.

To efficiently update IoT device applications at massive scale, technology vendors must leverage the cloud.

Vendors should create a trusted chain between device and cloud, with trust anchored at both ends. This means that the device network must also be secured by a root of trust. In so doing, trust is "baked" into the device and moves closer to the edge of the network. By enabling automatic device updates, rather than physically visiting devices, there are also potentially huge cost savings to be realized.

TIP

Lower costs are realized by reducing field call-outs for devices that haven't updated as desired in the campaign. Being able to remotely troubleshoot devices from afar can save hundreds, if not thousands, of dollars each time someone has to be sent into the field to access devices.

Security must be a cornerstone of any cloud-based update delivery service. The service must ensure secure delivery of authenticated and validated firmware to secure devices over multiple infrastructures and protocols that are essential for connected industrial operations. Because security elements are independent of transport protocol, the service must support a wide range of protocols. It should also support caching in the cloud environment. This feature enables users to bring update capability across a range of networks while saving money and improving flexibility. The service should also support encrypted update packages to protect intellectual property (IP) or to observe security licensing restrictions.

Further, updates across large deployments scaling millions or billions of devices can take a long time, and

power fluctuations or power outages during long update campaigns are all too common. Your update service requires robust software and hardware design and should support practical considerations for remote throttling and rollback protection. This feature prevents devices from being accidentally or maliciously rolled back to an older, more vulnerable firmware version.

WARNING

Factory and default settings on a device are popular targets for rollback attacks. You also need to ensure that your firmware and software updates don't restore any factory or default settings that may inadvertently make a previously secure device vulnerable.

Patching and Securing IoT Devices

Similar to the challenge of updating applications, the ability to quickly deploy security updates is necessary to ensure IoT devices operate securely and safely.

Security updates are typically smaller in size than application updates, but security updates must occur more frequently — and often quickly, to reduce exposure time when a new vulnerability is discovered.

Original equipment manufacturers (OEMs) typically ensure that security updates are delivered or made available to device owners and operators in the field.

Additionally, technology vendors and customers must be able to prove that security patches were properly installed, for regulatory compliance and due diligence purposes, with secure audit and logging capabilities.

Ensuring Scalability

Deploying application updates or security patches and remotely managing the operation and maintenance of many thousands of devices requires massive scalability and flexibility. For example, industrial and enterprise customers might need to leverage a system that delivers a consistent security model across gateway, on-premises, and private and public cloud environments.

By leveraging the cloud, some of these functions may be moved closer to the customer's edge network to provide compute, storage, and network resources that deliver the robust and scalable architecture required for a successful IoT deployment.

At the same time, it's important to have the choice to keep solutions on-premises, because many companies are loath to transition their legacy systems into the cloud, where their valuable data might be exposed.

Remotely connecting to a device helps technicians to quickly troubleshoot device or application issues, or train end-users in the operation of devices and applications.

Remote troubleshooting helps to correctly identify the root cause of an issue, so the right parts and/or field technician can be sent to the customer on the first trip.

Although a range of connectivity options are available, existing 4G LTE technology, bolstered by emerging 5G cellular connectivity, has the potential to become the primary choice for global, scalable IoT deployments. Therefore, consider how you intend to provision connected devices on a global scale across numerous borders, communications topologies, and mobile network operators (MNOs). Consider using embedded SIMs (eSIMs) that can be built into the device at the point of assembly and offer over-the-air (OTA) updates to provision new eSIM profiles remotely, without the cost of physically swapping the SIM for a new MNO in the field.

Managing Connectivity

Every connected IoT device is supported by a network connection that must be managed. This involves a series of significant considerations at every stage of establishing that connection. Considerations include:

- Subscriber lifecycle management
- Automated enrollment, validation, monitoring, and retirement of subscribers
- Connectivity technology selections

- A consolidated management interface for connectivity from multiple network operators
- Consolidated, accurate billing

Effective connectivity management is the combination of processes and tools that ensure these tasks are carried out in a consistent, coordinated, and scalable manner. By achieving this, every connection can be managed and secured throughout its lifecycle — from device onboarding, provisioning, and updates through to end-of-life decommissioning. Make sure your chosen solution enables global, scalable, and secure IoT deployments. For your company to realize these benefits, you should look for the following in a connectivity management solution:

- **Flexibility, simplicity, and cost-efficiency:** When evaluating candidate solutions for your business' specific needs, focus on these key requirements. Inadequacy in any of these areas will hamper your IoT projects or derail them entirely.
- **Consolidation:** Where connectivity management is concerned, your goal should always be a "single pane of glass." Give preference to candidate solutions that aggregate and consolidate device data, as well as cost and carrier relationship data, into actionable forms.
- **A trusted partner ecosystem:** When considering candidate solutions and providers, don't look only at the technologies they are offering. Connectivity management can directly affect, if not determine,

whether and how well your IoT projects meet your business goals. Look for a provider that combines superior technologies with experience, an ecosystem of partnerships, and commitment to the success of your business.

Maintaining Connectivity

In the industrial context, a remote device may be embedded in a harsh environment where access is limited. It may be buried next to a mast in a weatherproof case, and it may require technicians to travel hundreds of miles to repair. These devices may be deployed across a diverse network topology. Mechanisms designed for previous networked equipment may even be too constrained for IoT devices.

When considering the needs of teams responsible for managing and updating IoT devices, the success and return on investment (ROI) of IoT deployments depends on addressing questions like:

- How can I update my devices?
- What if a power outage during the update corrupts information on the device?

Support for a wide array of communications technologies and protocols is essential for maintaining connectivity under such challenging conditions.

IN THIS CHAPTER

- Addressing IoT security needs
- Building and maintaining trust

Chapter 4
Exploring Security and the Digital Social Contract

In this chapter, you learn why IoT resiliency and security risks must be addressed with greater urgency, and with a new approach by end-users and technology providers. This chapter also explores why a Digital Social Contract for Security is critical to building and maintaining a foundation of trust for the IoT.

Addressing Security

The world is witnessing cyberattacks on critical infrastructure, health services systems being held for ransom, and home electronics devices used as Internet gateways by hackers. The result, according to Lloyd's of London, is that cybercrime might be costing the global economy a half-trillion dollars a year because system and device security across all sectors are vulnerable to new attack methods.

The challenge of keeping systems secure has become a primary design consideration for the major technology companies. However, the risks to a system do not only lie with the hardware or software. Increasingly, cybercriminals are looking to circumnavigate built-in security through relatively simple social engineering techniques targeted at exploiting human vulnerabilities. Users are often the weakest link in secure systems.

As the interface between technology and human users becomes less distinct, and as the threats to personal safety become greater (for example, a hacked home security system that could be used to invade occupants' privacy), users must be their own first line of defense. This is true at a personal level as cybercriminals will continue to perpetrate identity theft and credit card fraud for the foreseeable future. It becomes even more important at the global level as cyberterrorists, competing nations, and hacktivists are likely to exploit the IoT to commit destructive and potentially lethal cyberattacks.

REMEMBER

Technology providers must embrace their own responsibilities with a Digital Social Contract for Security and endeavor to protect users — despite themselves — to create a foundation of trust.

TIP

Choose a platform that was built specifically for the IoT and features a security framework consisting of:

- A secure access point name (APN) gateway to route connectivity
- Device management features to ensure chip-to-cloud security
- Encryption of data at rest and in motion, with control over permissions and data access

Keeping a Social Contract

All technology companies' responsibilities under the Digital Social Contract are rising as connected devices proliferate. Cyberattackers are becoming increasingly sophisticated, so technology companies must continue to push security as a primary design consideration, ensuring that security defense scales with the threat. This Digital Social Contract will then form a foundation for explicit trust between the technology sector and all users.

Adherence to the Digital Social Contract will require companies to go well beyond the legal language in their terms and conditions, and regard robust security as a prerequisite in all design decisions. It will mean taking full account of how people are likely to use their technology, not how companies would like them to use it.

Although the Digital Social Contract also places a duty of care on users to protect themselves by behaving responsibly, technology designers will always carry the major burden because most end-users are not technology or security experts. It will require a swift departure from the mindset in which companies consider it acceptable, for example, to ship products with device passwords as simple as `12345` or `PASSWORD`.

The challenges in honoring the Digital Social Contract vary according to the area companies operate in. For example, the automotive industry is a 100-year-old sector going through immense disruption with the move to mass electric and hybrid fleets and autonomous vehicles.

Traditionally, automotive companies take seven to ten years to move from design to delivery. Today that innovation cycle is shrinking as they face competition from technology companies used to taking products to market much faster. It may be thought there is a possible risk that the Digital Social Contract could be damaged by such a disrupted competitive landscape. However, the automotive industry is governed by functional safety standards ensuring that vehicles meet stringent safety targets. In this case,

the Digital Social Contract is underpinned by a legal duty of care. So, while automakers are working out how to go faster, competitor technology companies are learning how to operate in a more highly regulated safety environment.

The risk to the Digital Social Contract is higher where time-to-market pressure is greatest. Security risks affect all markets but are potentially the most damaging in business markets and critical infrastructure because the fallout from an attack is likely to be higher.

Evidence of this growing threat came from the U.S. Department of Energy when it warned that electricity systems faced "imminent danger" from cyberattacks and threats were increasing in "sophistication, magnitude, and frequency."

In fast time-to-market segments, success is built on the model "design, ship, analyze, and pivot" — in other words, learning fast and iterating. But this approach can undermine robust security because weaknesses in products once they are deployed are harder to correct. Changing this model can be difficult in design-fast, iterate-fast markets where there might be a perception that best-practice security can affect schedule and the bottom line.

The way to change that perception, especially in a hot market like the IoT, is to remember that security is good for the bottom line and doesn't hurt time-to-market. This change will be possible by making secure-by-design technologies readily available to developers. This will

enable a new business model built for the IoT, one that aligns perfectly with Social Contract responsibilities.

The new model will make it harder to breach chip security and allow more time for system defenses to react. This model can be summarized as:

- Design for security
- Ship
- Analyze
- Self-heal or quarantine
- Treat (if required)

This model will be crucial in segments like the IoT with the potential for vast numbers of deployed, connected devices in a single system. It will provide a more complex model protecting system integrity, and ensure the technology sector takes lifecycle responsibility for products.

This model covers the ability to patch devices en masse, such as with smartphone bug fixes. The evolution will also bring the capability to quarantine single devices until they can be rehabilitated.

The key to this new business model is distributed intelligence. It means pushing the kind of powerful compute capability now found mainly in the cloud to the edge of the device network. This will move organizations to a more flexible, dispersed security model.

IN THIS CHAPTER

- Managing and updating at scale
- Staying connected
- "Future-proofing" your solution
- Improving security

Chapter 5
Ten Principles of a Successful IoT Deployment

This chapter provides ten key principles to help you design a successful IoT solution:

- Ensure post-deployment management and maintenance capabilities at massive scale, and define a complete deployment-to-obsolescence device lifecycle management plan.

- Plan and design for robust connectivity in harsh, isolated operating environments, and define resilience and safety requirements.
- Recognize that one size does not fit all. Power (battery life), size, network connectivity, and reliability are crucial in IoT systems.
- Leverage a proven ecosystem for flexibility and choice, and to help "future-proof" your solution.
- Identify a robust commercial business plan, including building a complete use case for how you plan to leverage the data you want to capture.
- For sensitive data running on legacy systems, consider an on-premises solution that delivers management and monitoring capabilities within your firewall.
- Use standard security building blocks to ensure chip-to-cloud security, which are inherently more secure because of industry review and upkeep. These blocks are more reliable because they don't require you to change your systems later when the non-standard blocks go away.
- Make designs more compartmentalized to better isolate and wall off cyberattacks.
- Use hardware-based root-of-trust security to provide essential security services and protect critical code, data, and hardware.
- Use the Digital Social Contract for IoT security as the foundation for long-term trust between technology providers and users.

Step into the IoT future

The Internet of Things (IoT) is creating a global network of connected, intelligent devices that will inform and enhance society and business. Many important challenges and design considerations must be addressed early to build a complete and secure IoT solution. This book shows what is required to design a robust, scalable IoT solution serving a range of markets and needs, including important challenges to consider and why it is vital to address those challenges at the earliest stages of planning and design.

Inside…

- Explore IoT market opportunities
- Consider design choices
- Manage and update at scale
- Design for robust connectivity
- Protect code, data, and hardware

arm

Lawrence C. Miller has worked in information technology for more than 25 years. He has written more than 60 *For Dummies* books.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-65675-3
Not For Resale

for dummies® A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.