Internet of Things (IoT) Rollouts in the Telehealth Industry

Himanshu Shah

Editor's note: Mr. Shah has contributed a detailed analysis of considerations consistent with a successful rollout of IoT (Internet of Things). It is essential reading for anyone involved in establishing inter-networking of physical devices. Caution: for the novice, the use of acronyms may be overwhelming, leading one to mistakenly conclude that this information is more than anyone might want to know about IoT. To aid in understanding and eventual application of this information, a glossary is appended to this article.

Many enterprises are considering, or are already, deploying Internet of Things (IoT) solutions,[1] but IoT deployments have seen a dark side; one where implementation is partially completed or unsuccessful, which kills the business case driver.[2] This article reviews the challenges one might experience and how to mitigate them.

What is Internet of Things?

The Internet of Things is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data.

IoT in the Telehealth Industry

Telehealth is essentially remote monitoring of patient health data wherever the patient might be. Predominantly, the patient is in their home, elderly, and suffering from a long-term condition or chronic disease. Increasingly, telehealth is allowing citizens of all ages to take control of their well-being and understand what is happening to them physiologically so they can lead a better, healthier life. The development of telehealth has grown from a system meant to monitor vital health data, into one where active citizens are becoming more aware of their lifestyle and its effect on their health.

People with chronic diseases, such as chronic obstructive pulmonary disease (COPD), diabetes, and heart failure are most at risk of complications if they aren't monitored regularly. In the developed world, these three diseases are the top three reasons for urgent assessment and admission into an emergency department or hospital.

Considerations for Successful Implementation of IoT

Deployment, readiness, and maintenance are all part of successful implementation.

Deployment Sites

As IoT devices in telehealth are usually deployed at patients' homes or remote, unknown customer locations, it is important to perform site surveys of field conditions, such as room condition, range of the IoT devices to other medical devices, as well as cellular and Wi-Fi availability and signal strength.

Inaccurate and irrelevant details captured by the field staff can lead to inaccurate planning resulting in surprises when technician/deployment teams arrive on site for installation and deployment. Every site is dynamic in terms of room layouts, network conditions, power availability, and access to quality local support staff. Therefore, the personnel conducting site surveys must know the overall solution planned, with analytical ability to probe and capture relevant information about site conditions. This will lead to more efficient rollouts.

Care Innovations® (which offers turnkey remote patient management solutions) proposes capturing site conditions using digitized site details via relevant photos. Analyzing site data before installation is always helpful for program implementation success.

It is equally important to update data, post rollout, to fill gaps in initial site surveys and assist post rollout support teams.

Site Readiness: Keeping Key Stakeholders Informed

The rollout of IoT devices on-site usually has a huge dependency on customers for site readiness. Gaps in communication between management and their on-site personnel lead to last minute surprises. This might include delays or unavailability of network connectivity, power points, installation space, cabling duct access, and permissions for device-related cabling. Additionally, unavailability of key local support staff (e.g., electricians, networking staff, and other administration staff) can be showstoppers to rollout and support activities. Field engineers usually face the brunt and often face resistance for installations on site, leading to delays in installation.

Maintenance Challenges

1) IoT devices are machines, and sometimes they fail. Aligning downtime for servicing devices on site can be a challenge, especially for areas that are customer-facing (e.g., hospitals, nursing facilities). Due to the potentially sensitive impact on servicing customers, such unplanned delays cannot be avoided, requiring service personnel to be on call, or even forced to schedule

service calls during non-business hours. Managing SLA's (service area agreements) under such scenarios could be a challenge.

2) Deployment of IoT devices is often done in remote areas that may be hazardous for normal human operations. Such areas may have statutory dependency on certified personnel for deployment and interfacing with hazardous equipment. Availability of these specialized skills may be limited during unscheduled downtimes. Factoring for the costs for paying specialized technicians (e.g., electricians, carpenters) is often underestimated during the commercial stage, leading to cost overhead during installation and support.

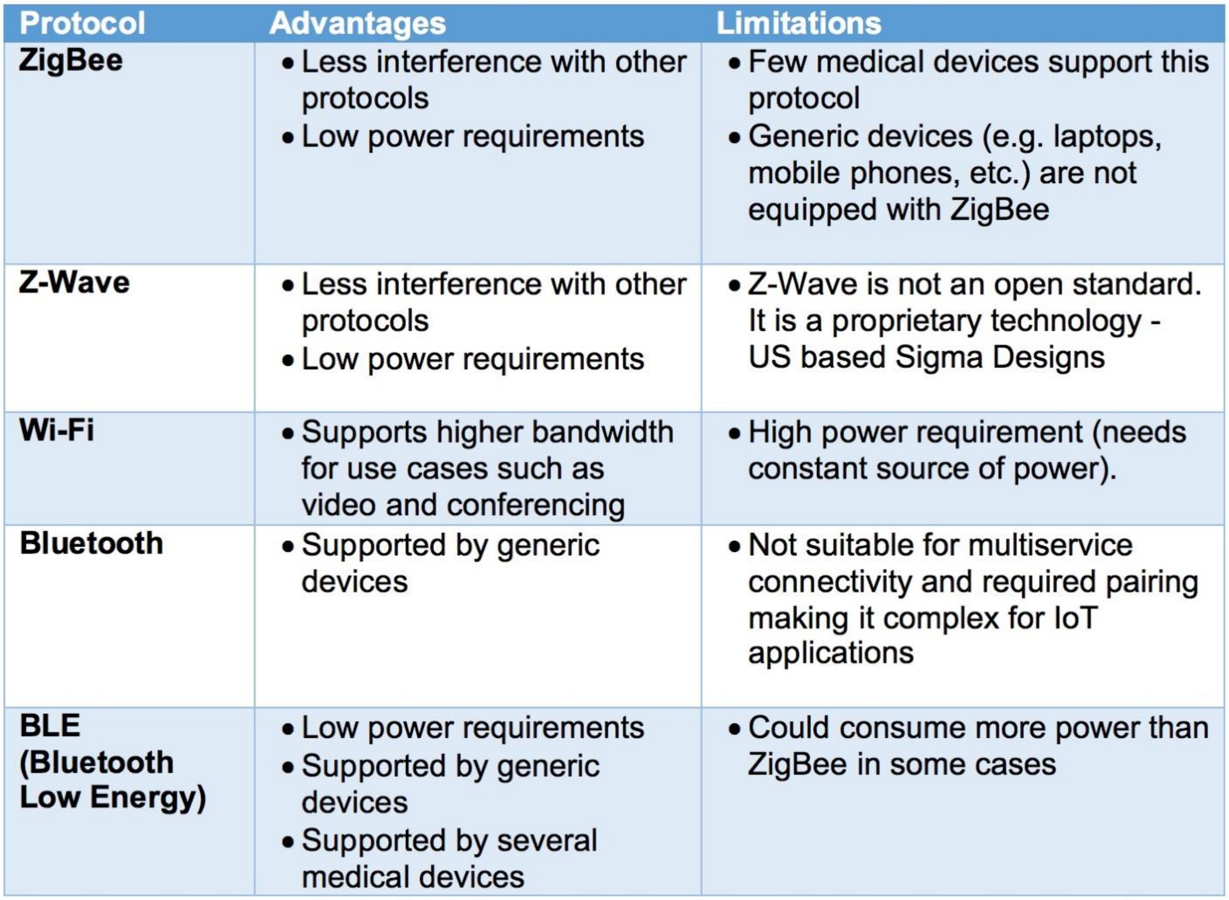
IoT Device Selection

The components of IoT selection include, communication protocols, network connectivity and selection, and hardware grade selection.

Protocol Selection

Several protocols for device connectivity are available. The IoT hub must support the right protocol(s) for device connectivity. Table 1 details the advantages and limitations of popular protocols in this space.

Table 1. The IoT hub must support the right protocol(s) for device connectivity. Listed here are advantages and limitations of popular protocols.

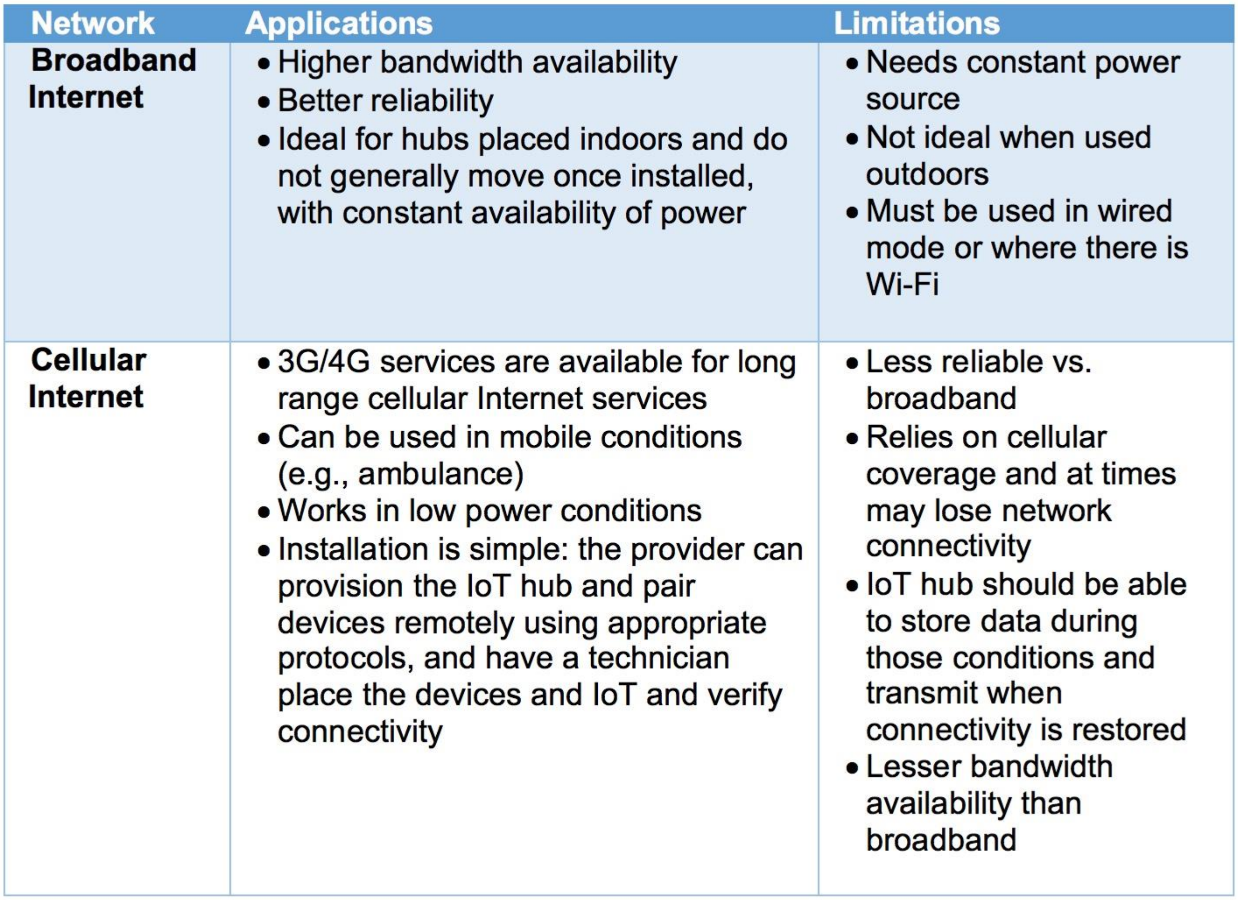


Protocol	Advantages	Limitations
ZigBee	• Less interference with other protocols • Low power requirements	• Few medical devices support this protocol • Generic devices (e.g. laptops, mobile phones, etc.) are not equipped with ZigBee
Z-Wave	• Less interference with other protocols • Low power requirements	• Z-Wave is not an open standard. It is a proprietary technology - US based Sigma Designs
Wi-Fi	• Supports higher bandwidth for use cases such as video and conferencing	• High power requirement (needs constant source of power).
Bluetooth	• Supported by generic devices	• Not suitable for multiservice connectivity and required pairing making it complex for IoT applications
BLE (Bluetooth Low Energy)	• Low power requirements • Supported by generic devices • Supported by several medical devices	• Could consume more power than ZigBee in some cases

Network Connectivity Selection

One must also ensure the correct selection of network connectivity for the IoT hub to support. Based on the application, it might not be possible for a hub to support multiple network options due to cost, size, and security reasons. Table 2 lists the application areas and limitations of popular network connectivity options.

Table 2. Application areas and limitations of popular network connectivity options.

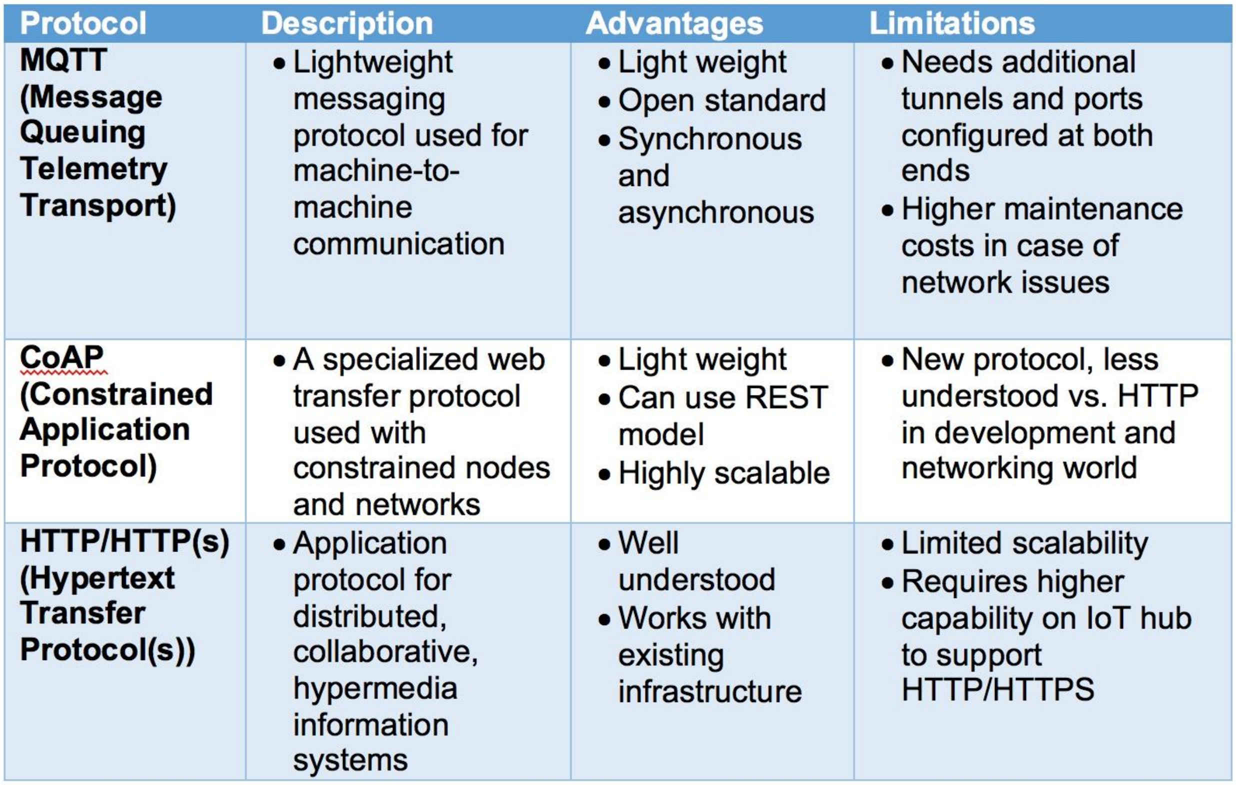


Network	Applications	Limitations
Broadband Internet	• Higher bandwidth availability • Better reliability • Ideal for hubs placed indoors and do not generally move once installed, with constant availability of power	• Needs constant power source • Not ideal when used outdoors • Must be used in wired mode or where there is Wi-Fi
Cellular Internet	• 3G/4G services are available for long range cellular Internet services • Can be used in mobile conditions (e.g., ambulance) • Works in low power conditions • Installation is simple: the provider can provision the IoT hub and pair devices remotely using appropriate protocols, and have a technician place the devices and IoT and verify connectivity	• Less reliable vs. broadband • Relies on cellular coverage and at times may lose network connectivity • IoT hub should be able to store data during those conditions and transmit when connectivity is restored • Lesser bandwidth availability than broadband

Communication Protocol Selection

The IoT hub is generally responsible for collecting data from various devices and transmitting the data to a central infrastructure, such as a cloud server. (With cloud hosting, clients rent virtual server space rather than renting or purchasing physical servers.)[1] The next important things to consider are communication protocol options between the hub and the cloud infrastructure (Table 3).

Table 3. Communication protocol options between the hub and the cloud infrastructure.



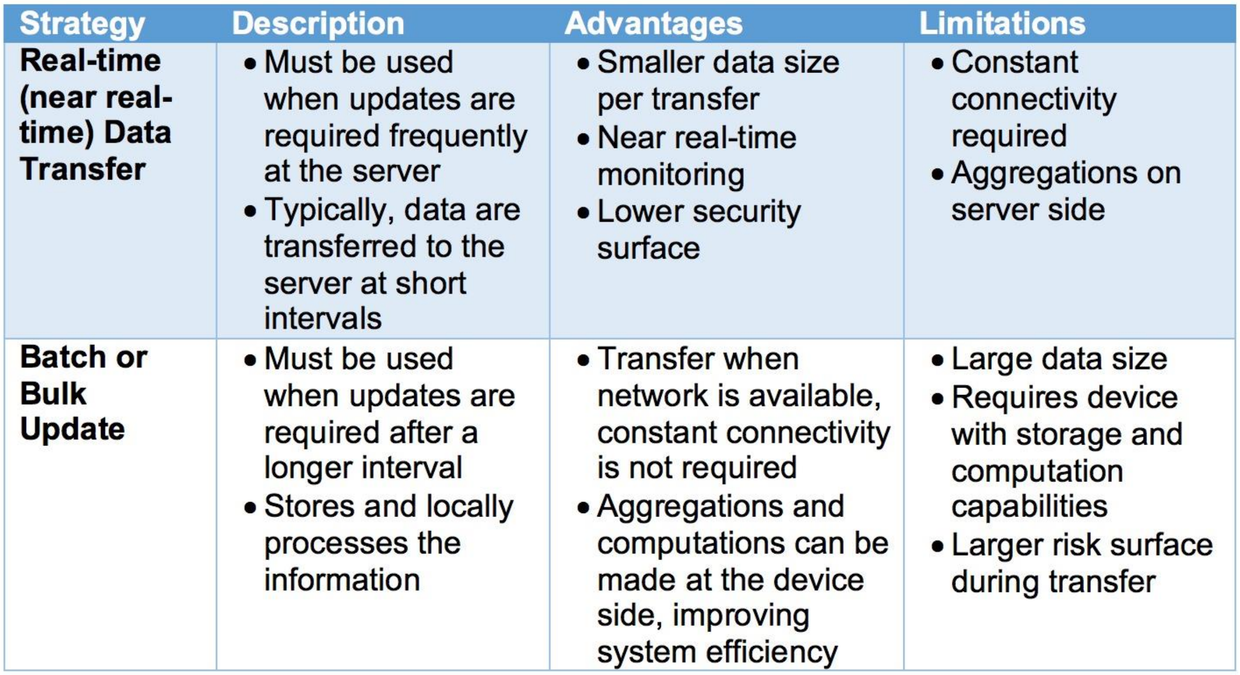
Protocol	Description	Advantages	Limitations
MQTT (Message Queuing Telemetry Transport)	• Lightweight messaging protocol used for machine-to-machine communication	• Light weight • Open standard • Synchronous and asynchronous	• Needs additional tunnels and ports configured at both ends • Higher maintenance costs in case of network issues
CoAP (Constrained Application Protocol)	• A specialized web transfer protocol used with constrained nodes and networks	• Light weight • Can use REST model • Highly scalable	• New protocol, less understood vs. HTTP in development and networking world
HTTP/HTTP(s) (Hypertext Transfer Protocol(s))	• Application protocol for distributed, collaborative, hypermedia information systems	• Well understood • Works with existing infrastructure	• Limited scalability • Requires higher capability on IoT hub to support HTTP/HTTPS

HTTP: Hypertext Transfer Protocol; HTTPS: Hypertext Transfer Protocol Secure; REST: Representational state transfer

Communication Strategy Selection

Once the communication network and protocol are in place, the right selection of the communication strategy must be performed. This should be done based on how frequently updates are required, security, cost, and network constraints. The two main strategies are summarized in Table 4.

Table 4. Options for Communications.



Strategy	Description	Advantages	Limitations
Real-time (near real-time) Data Transfer	• Must be used when updates are required frequently at the server • Typically, data are transferred to the server at short intervals	• Smaller data size per transfer • Near real-time monitoring • Lower security surface	• Constant connectivity required • Aggregations on server side
Batch or Bulk Update	• Must be used when updates are required after a longer interval • Stores and locally processes the information	• Transfer when network is available, constant connectivity is not required • Aggregations and computations can be made at the device side, improving system efficiency	• Large data size • Requires device with storage and computation capabilities • Larger risk surface during transfer

Hardware Grade Selection

Internet of Things hubs are exposed to a range of environmental conditions depending on where they are deployed and used. It is very important to identify these conditions during the design phase and select the correct grade: commercial, medical, industrial, and military. A lower grade selection could lead to failure of the product while a higher selection may result in cost overruns. Hence, make the right selection at the design phase to develop the hub.

These products and components vary in the following key factors:

1. NAND flash memory (a storage technology that does not require power to retain data)
2. Controller design characteristics
3. Firmware algorithms
4. Write endurance
5. Cost

6. Supported temperature ranges
7. Controlled BOM (bill of materials; a list of materials, needed to manufacture a product)
8. Product life-cycles
9. Power protection
10. Product change notification (PCN) policy (a document issued by a manufacturer informing customers about a product change)
11. Unexpected power interrupt handling
12. Mean time between failure (MTBF; a measure of hardware reliability)

Security

Internet of Things devices generally transmit data over the Internet, with data stored in an infrastructure, such as a cloud. A medical IoT system could contain sensitive information, such as PHI (Patient Health Information) and PII (Patient Identity Information). This information must be protected during transmission and at rest. Security must be built by design and not as an afterthought.

Security During Transmission

During transmission of information, security must be designed for at four levels: gateway, channel, message, and data. Strategies, such as bi-directional fingerprinting, must be used to ensure that the device is transmitting to the right server and the server is receiving data from a valid device.

When information is at rest, it may be stored in a relational database system or big data systems. One must make sure of the following: encryption of sensitive information in the data stores, sensitive information is stored in security-certified data centers, and access to the information systems and data system are controlled. Keep in mind that security adds performance and cost overheads, it must be designed optimally.

Device Testing and Support

Issues in this aspect of IoT include connectivity, lifecycle management, logistics, and inventory management. Inadequate experience in on-field issues may lead to design flaws and inadequate testing of field conditions not envisaged for error handling and self-healing. To compound this, compromising testing time after last minute design changes due to haphazard business inputs leads to less roadworthy releases. These releases are highly prone to costly re-work or device recalls from the field. One of the biggest handicaps of field personnel is the lack of knowhow and non-availability of specialized equipment and back-office support channels required to troubleshoot issues on site. This can result in unplanned logistic costs and efforts leading to customer dissatisfaction due to snowballing turn-around-times.

Sensors subject to heat, cold, shock, humidity, etc., during storage, shipment and/or assembly, may show a change in response. Choice of rugged and reliable sensors that can withstand harsh environmental conditions on field ensure reliability of the overall solution. Regular calibration of sensors ensures reliability of data captured by sensors on field over time.

Testing should also account for weak Wi-Fi signals, low cellular coverage areas, environmental conditions changes, and other electronic devices in close proximity.

Connectivity Demons

“CONNECTIVITY” is the reason for the existence of IoT. A sustainable IoT solution must ensure that a reliable cellular coverage or data communication channel is always present between the device and the backend systems to support monitoring and provide analytics. Issues, such as a lack of cellular coverage at locations where IoT devices are deployed plague IoT implementations, with the discovery that SIM cards that work fine in the lab may not necessarily work at a site. This may be due to factors, such as inadequate cellular signal strength inside buildings, the telecom provider not having coverage in the cellular circles, signal jamming, or electrical interference. Choose a telecom service provider that has the best network coverage at a site.

IoT devices that rely on internet gateway via existing LAN (local area network) or Wi-Fi networks often face issues of network blackout due to multiple reasons, including wire cuts, network infrastructure failure, inexperienced field support or customer networking support staff. Third-party service providers are most commonly relied on to fix these issues. Network or periphery firewall issues and a lack of quantifiable SLA's often hamper resolution times. The need to align SLA's to support business criticality of dependent processes is crucial.

Device Lifecycle Management

An IoT device has a lifecycle. Once a device is provisioned into operation, it goes through several states: activation, inactivation, reassignment to a new user, a new software or configuration update, and retirement. The lifecycle depends on the specific use. The status may need a workflow involving human interactions (e.g., an approval). A device’s lifecycle must be thought out and integrated into the system design phase. If not, this might lead to many operational issues, such as how data for an old user are managed when the same device is assigned to a new user, or issues concerning what the server should do when a deactivated device transmits information.

Logistics and Inventory Management

Inadequate logistics coverage to remote locations where devices are to be deployed leads to transit delays from courier agencies. Non-availability of relevant recipients at the point of delivery can lead to delays in receipt at sites. Large IoT rollouts across multiple sites must have strong inventory tracking and device provisioning systems. Inaccurately captured device ID's lead to poor inventory tracking during post-rollout maintenance and support, especially during reverse logistics for device replacement and repair. Adequate support of taxation and finance teams ensure compliance with statutory documentations to take care of nuances of tax laws during transportation to each state. The lead-times and costs required for these statutory documentations and logistics must be factored as part of the rollout and support planning.

Conclusion

Many challenges confront IoT deployment. With proper understanding of these challenges and thorough and proactive planning, organizations can achieve successful and efficient rollouts.

Reference

1. What are cloud servers. Interoute. 2017. URL: http://www.interoute.com/what-are-cloud-servers. Accessed 5/17/17.

Himanshu Shah serves as Care Innovations®' Chief Information Officer. He is a member of the executive leadership team, which sets product and architectural strategic direction. In his role, he leads the company's information technology team, who is responsible for setting product technology plans and delivering all technology services. Those services include integration, mobile development, analytics, quality assurance, support and maintenance, as well as infrastructure and security management. Mr. Himanshu has transformed the company's information technology structure by achieving new levels of efficiency and positioning Care Innovations for organic and explosive growth, all the while sustaining the company's goal to provide patients with high-quality remote care at an affordable cost.

Glossary

Batch and bulk update: Allows setting a property on many objects in one operation.

BIND (Bi-Directional Fingerprinting): Traffic exchanged in the two directions of a connection depend upon each other. Therefore, a bi-directional fingerprinting mechanism leverages this sequence dependence.

BOM (Build of Materials): A list of the raw materials, sub-assemblies, intermediate assemblies, sub-components, parts and the quantities of each needed to manufacture a product.

Cloud: Cloud storage is a model of data storage in which digital data are stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company.

CoAP (Constrained Application Protocol): A specialized web transfer protocol for use with constrained nodes and constrained networks

HTTP (Hypertext Transfer Protocol): The underlying protocol used by the World Wide Web, which defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

IoT Hub: Mediates the interactions between your device and your solution back end. The goal is to establish trustworthy, bidirectional communication paths between a control system, such as IoT Hub and special-purpose devices that are deployed in untrusted physical space.

IoT: “The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention.”

LAN (Local Area Network): a network that links two or more devices using a wireless distribution method within a limited area such as a home, school, computer laboratory, or office building.

MQTT (Message Queuing Telemetry Transport): A lightweight messaging protocol used for machine-to-machine communication

MTBF (Mean time between failure): A measure of how reliable a hardware product or component is. For most components, the measure is typically in thousands or even tens of thousands of hours between failures. For example, a hard disk drive may have a mean time between failures of 300,000 hours.

NAND flash memory: A type of non-volatile storage technology that does not require power to retain data. An important goal of NAND flash development has been to reduce the cost per bit (short for binary digit—the smallest unit of data in a computer) and increase maximum chip capacity so that flash memory (a kind of memory that retains data in the absence of a power supply) can compete with magnetic storage devices like hard disks.

PCN (Product Change Notification): An announcement that informs customers of change.

PHI (Patient Health Information): The Federal government requires organizations to identify protected health information and handle it securely.

PII (Patient Identity Information: The Federal government requires organizations to identify personally identifiable information and handle it securely.

SIM (Subscriber Identity Module) card: A small circuit board in most modern phones that communicate with the carrier. Practically speaking, it is a middleman between two pieces of hardware: the phone's baseband chip and the carrier's cell towers, allowing the two to communicate.

SLA’s (Service Area Agreements): A contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the performance standards the provider is obligated to meet.

Wi-Fi (Wireless Fidelity): A facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

References

1. Cha, B. A beginner’s guide to understanding to Internet of Things. Recode. 2015. URL: https://www.recode.net/2015/1/15/11557782/a-beginners-guide-to-understanding-the-internet-of-things. Accessed: 3/30/17.

2. Leonard M. When the IoT becomes an agent of the dark side. GCN. 2016. URL: https://gcn.com/articles/2016/10/28/iot-botnet.aspx?admgarea=TC_SecCybersSec. Accessed: 3/30/17.

Department: Research and Innovation

Tags: Batch and bulk update, BIND (Bi-Directional Fingerprinting), BOM (Build of Materials), Cloud, CoAP (Constrained Application Protocol), HTTP (Hypertext Transfer Protocol), Internet of Things, IoT (Internet of Things), IoT Hub, LAN (Local Area Network), MQTT (Message Queuing Telemetry Transport), MTBF (Mean time between failure), NAND flash memory, PCN (Product Change Notification), PHI (Patient Health Information), PII (Patient Identity Information), SIM (Subscriber Identity Module) card, SLA’s (Service Area Agreements), Wi-Fi (Wireless Fidelity)