ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The Architecture and Challenges Issues in IOT

L.V.Satyanarayana
Assistant Professor,
Aditya institute of Technology and Management,
Tekkali.

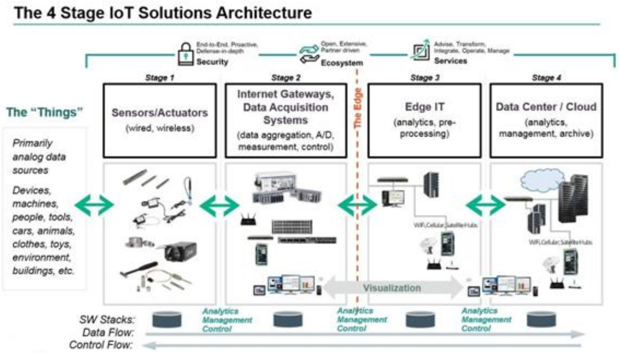
V.Ashok Gajapathi Raju
Assistant Professor,
Aditya institute of Technology and Management,
Tekkali.

Abstract:

The IoT is more than Internet-connected consumer devices. Sooner or later, your IT organization will need you to create an infrastructure to support it. Energy companies already use networked sensors to measure vibrations in turbines. They feed that data through the network to computing systems that analyze it to predict when machines will need maintenance and when they will fail. Jet engine manufacturers embed sensors that measure temperature, pressure, and other conditions to improve their products. Even a gift basket business can deploy sensors to constantly monitor the temperature of perishable products. If temperatures in storage or in transit start to rise, they can expedite deliveries. This has the dual advantage of increasing customer satisfaction while avoiding product spoilage.

The four-stage architecture of an IoT system

Stage 1 of an IoT architecture consists of your networked things, typically wireless sensors and actuators. Stage 2 includes sensor data aggregation systems and analog-to-digital data conversion. In Stage 3, edge IT systems perform preprocessing of the data before it moves on to the data center or cloud. Finally, in Stage 4, the data is analyzed, managed, and stored on traditional back-end data center systems. Clearly, the sensor/actuator state is the province of operations technology (OT) professionals. So is Stage 2. Stages 3 and 4 are typically controlled by IT, although the location of edge IT processing may be at a remote site or nearer to the data center. The dashed vertical line labeled "the edge" is the traditional demarcation between OT and IT responsibilities, although this is blurring. Here's a look at each in detail.


The 4 Stage IoT Solutions Architecture
End-to-End, Proactive, Defense-in-depth
Security
Open, Extensive, Partner driven
Ecosystem
Advise, Transform, Integrate, Operate, Manage
Services
Stage 1
Stage 2
Stage 3
Stage 4
The "Things"
Primarily analog data sources
Devices, machines, people, tools, cars, animals, clothes, toys, environment, buildings, etc.
Sensors/Actuators (wired, wireless)
Internet Gateways, Data Acquisition Systems (data aggregation, A/D, measurement, control)
The Edge
Edge IT (analytics, pre-processing)
Data Center / Cloud (analytics, management, archive)
WiFi,Cellular,SatelliteHubs
Visualization
SW Stacks:
Data Flow:
Control Flow:
Analytics Management Control
Analytics Management Control
Analytics Management Control

Stage 1. Sensors/actuators

Sensors collect data from the environment or object under measurement and turn it into useful data. Think of the specialized structures in your cell phone that detect the directional pull of gravity—and the phone's relative position to the "thing" we call the earth—and convert it into data that your phone can use to orient the device. Actuators can also intervene to change the physical conditions that generate the data. An actuator might, for example, shut off a power supply, adjust an air flow valve, or move a robotic gripper in an assembly process. The sensing/actuating stage covers everything from legacy industrial devices to robotic camera systems, water-level detectors, air quality sensors, accelerometers, and heart rate monitors. And the scope of the IoT is expanding rapidly, thanks in part to low-power wireless sensor network technologies and Power over Ethernet, which enable devices on a wired LAN to operate without the need for an A/C power source. In an IoT architecture, some data processing can occur in each of the four stages. However, while you can process data at the sensor, what you can do is limited by the processing power available on each IoT device. Data is at the heart of an IoT architecture, and you need to choose between immediacy and depth of insight when processing that data.

The more immediate the need for information, the closer to the end devices your processing needs to be.

For deeper insights that require more extensive processing, you'll need to move the data into a cloud- or data center-based system that can bring several sources of data together. But some decisions simply can't wait for deep processing. Did the robotic arm performing the surgery cut an artery? Will the car crash? Is the aircraft approaching the threat detection system a friend or a foe? You don't have time to send that data to your core IT assets. You must process the data right at the sensor— at the very edge of the edge network—for the fastest response.

Stage 2. The Internet gateway

The data from the sensors starts in analog form. That data needs to be aggregated and converted into digital streams for further processing downstream. Data acquisition systems (DAS) perform these data aggregation and conversion functions. The DAS connects to the sensor network, aggregates outputs, and performs the analog-to-digital conversion. The Internet gateway receives the aggregated and digitized data and routes it over Wi-Fi, wired LANs, or the Internet, to Stage 3 systems for further processing. Stage 2 systems often sit in close proximity to the sensors and actuators. For example, a pump might contain a half-dozen sensors and actuators that feed data into a data aggregation device that also digitizes the data. This device might be physically attached to the pump. An adjacent gateway device or server would then process the data and forward it to the Stage 3 or Stage 4 systems. Why preprocess the data? The analog data streams that come from sensors create large volumes of data quickly. The measurable qualities of the physical world in which your business may be interested—motion, voltage, vibration, and so on—can create voluminous amounts of constantly changing data. Think how much sensor data a complex machine like an aircraft engine might generate in one day, and there's no theoretical limit to the number of sensors that could be feeding data into an IoT system. What's more, an IoT system is always on, providing continuous connectivity and data feeds. IoT data flows can be immense—I've seen as much as 40 TB/second in one case. That's a lot of data to transport into the data center. It's best to preprocess it. Another reason not to pass the data on to the data center in this form is that analog data has specific timing and structural characteristics that require specialized software to process. It's best to convert the data into digital form first, and that's what happens in Stage 2. Intelligent gateways can build on additional, basic gateway functionality by adding such capabilities as analytics, malware protection, and data management services. These systems enable the analysis of data streams in real time. Although delivering business insights from the data is a little less immediate at the gateway than it would be when sent directly from the sensor/actuator zone, the gateway has the compute power to render the information in a form that is more understandable to business stakeholders. Gateways are still edge devices—they're external to the data center—so geography and location matter. In the pump example, if you have 100 pump units and want to process data on-premises, you might have instant data at the pump level, aggregate the information to create a plantwide view for the facility, and pass the data on to the data center for companywide view. DAS and gateway devices may end up in a wide variety of environments, from the factory floor to mobile field stations, so these systems are usually designed to be portable, easy to deploy, and rugged enough to withstand variations in temperature, humidity, dust, and vibration.

Stage 3. Edge IT

Once IoT data has been digitized and aggregated, it's ready to cross into the realm of IT. However, the data may require further processing before it enters the data center. This is where edge IT systems, which perform more analysis, come into play. Edge IT processing systems may be located in remote offices or other edge locations, but generally these sit in the facility or location where the sensors reside closer to the sensors, such as in a wiring closet.

Because IoT data can easily eat up network bandwidth and swamp your data center resources, it's best to have systems at the edge capable of performing analytics as a way to lessen the burden on core IT infrastructure. If you just had one large data pipe going to the data center, you'd need enormous capacity. You'd also face security concerns, storage issues, and delays processing the data. With a staged approach, you can preprocess the data, generate meaningful results, and pass only those on. For example, rather than passing on raw vibration data for the pumps, you could aggregate and convert the data, analyze it, and send only projections as to when each device will fail or need service.

Stage 4. The data center and cloud

Data that needs more in-depth processing, and where feedback doesn't have to be immediate, gets forwarded to physical data center or cloud-based systems, where more powerful IT systems can analyze, manage, and securely store the data. It takes longer to get results when you wait until data reaches Stage 4, but you can execute a more in-depth analysis, as well as combine your sensor data with data from other sources for deeper insights. Stage 4 processing may take place on-premises, in the cloud, or in a hybrid cloud system, but the type of processing executed in this stage remains the same, regardless of the platform.

Challenges to IOT Security Concerns –

With so many interconnected devices out there in market and plenty more to come in the near future, a security policy cannot be an afterthought. If the IOT devices are poorly secured, cyber attackers will use them as entry points to cause harm to other devices in the network. This will lead to loss of personal data out into the public and the entire trust factor between internet connected devices and people using them will deteriorate. In order to evade such scenarios, it's extremely critical to ensure the security, resilience and reliability of internet applications to promote use of internet enabled devices among users across the world. Security constraints for IOT are so critical that even analyst firm Gartner came out with some astounding numbers. According to them, the worldwide spend for the IoT security market will reach $348 million in 2016, a rise of 23.7% from $281.5 million in 2015.

Privacy issues –

The possibility of tracking and surveillance of people by government and private agencies increases as the devices are constantly connected to the internet. These devices collect user data without their permission, analyze them for purposes only known to the parent company. The social embrace of the IOT devices leads people to trust these devices with collection of their personal data without understanding the future implications.

Inter-Operatability Standard Issues –

In an ideal environment, information exchange should take place between all the interconnected IoT devices. But the actual scenario is inherently more complex and depends on various levels of communication protocols stacks between such devices. The OEM's producing industry ready IoT devices will need to invest a lot of money and time to create standardized protocols common for all IoT devices or else it will delay product deployment across different verticals.

Legal Regulatory and Rights Issues –

There are no concrete laws present which encompasses the various layers of IoT across the world. The gamut of devices connected to each other raises many security issues and no existing legal laws address such exposures. The issues lie in whether current liability laws will extend their arm for devices which are connected to the internet all the time because such devices have complex accountability issues.

Emerging Economy and Development Issues –

IoT provides a great platform for enablement of social development in varied societies across the world and with the proliferation of Internet across the various sections of the society in developing countries coupled with lowering costs of microprocessors and sensors will make IoT devices accessible to low income households. But there are lot of shortcomings related to enablement of high speed internet and basic technology services architecture for commercial and business usage in developing countries. Until and unless, a basic infrastructure is in place, devices would be of no value to the users. While IoT brings about new opportunities; at the same time, it adds multiple layers of complexity. Such a new environment of devices will add a new dimension for policy makers in emerging economies who will need to chalk out a new blueprint for IoT related regulatory concerns. The future lies in interconnected devices but how we manage them will decide how our Digital future is shaped.

New Use Cases

Remember when the personal computer first emerged, and it was promoted as a place to store recipes? Or when the iPad was released and articles suggested how it might be used? Like the personal computer and the iPad, the IoT is one of those ideas that is being developed because it is possible, not because it can fulfill any specific problem. Although examples of how to use the IoT usually involve timers for turning appliances on and off, the real purposes will probably emerge only after smart devices are everywhere. That does not mean that the IoT won't be a success, or revolutionize technology. However, it does mean that its consequences are difficult to foresee. Advising everyone to expect the unexpected is probably the only reliable advice -- and that suggestion is hardly accurate for long range planning.

The Need for Open Standards

The IoT consists of a lot of individual devices with their own specifications. At this stage, that hardly matters, but a time will arrive soon when further growth will require that smart devices can communicate with each other. Yet, although much of the IoT is likely to be built with open source software, universal standards and protocols lag behind the development of smart technology. The few efforts that exist tend to be specific to a technology, such as Eclipse IoT, and tend to focus on applying existing standards or protocols to smart devices rather than being developed for the new demands of the IoT. Without a greater degree of cooperation, the growth of the IoT is to be slower than it could be.

Energy Demands

Several years ago, Gartner predicted that 4.9 billion smart devices would be used by 2015 -- an increase of thirty percent from 2030. By 2020, Gartner estimated that the number of smart devices would reach 25 billion by 2020, an increase of 100% each year. Along with this boost will come an increase in energy demands comparable to the one created by the Internet. In 2012, the data centers that powered the Internet were estimated to require 30 billion watts of electricity a year -- enough to power a medium-sized town, and the Internet of Things is likely to require even more.
Even with improved batteries and green sources like solar and wind, just meeting the demand will be difficult. However, add issues like the wasted energy and pollutants, and powering the IoT could become a major social problem in its own right within the next decade.

Storage Issues

Storage of information generated by smart devices will increase the energy demands required by the Internet of Things. A single corporation like Google, which already has myriad server farms, each occupying tens of thousands of square feet, could be dwarfed by the demands of smart devices. However, the physical demands are only part of the problem. Much of the data generated by smart devices is needed only briefly to send signals to device, and does not need to be stored. Other data, such as timers for devices, might ordinarily need to be stored for only a week or two at the most. Yet with such information being available, the demand may arise for storing part of this surge of information for longer periods. Consequently, policies will be needed about what kind of information is stored, and for how long -- to say nothing of who can access it, and the exceptions that might be made to whatever general policies are devised.

References:

1. http://www.microwavejournal.com/articles/27690-addressing-the-challenges-facing-iot-adoption
2. https://blog.apnic.net/2015/10/20/5-challenges-of-the-internet-of-things/
3. https://www.sitepoint.com/4-major-technical-challenges-facing-iot-developers/
4. https://www.linkedin.com/pulse/iot-implementation-challenges-ahmed-banafa?trk=mp-author-card
5. https://www.linkedin.com/pulse/why-iot-needs-fog-computing-ahmed-banafa?trk=mp-author-card
6. http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html