International Journal of Engineering Research and General Science Volume 4, Issue 3, May-June, 2016
ISSN 2091-2730

Internet of Things: Challenges and impact

Prof. Parul Wadhwa, Prof. Anu Puri

Asstt. Prof. (ECE) NHCE,Bangalore

parulwadhwa5@gmail.com, anu.puri2015@gmail.com

Abstract— IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), microservices and the Internet. The convergence has helped tear down the silo walls between operational technology (OT) and information technology (IT), allowing unstructured machine-generated data to be analyzed for insights that will drive improvements.

Practical applications of IoT technology can be found in many industries today, including precision agriculture, building management, healthcare, energy and transportation.

Keywords— internet of things, hype cycle, embedded software, big data, accurate computation, IoT business solution, real time analytics .

INTRODUCTION

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction

A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

Kevin Ashton, cofounder and executive director of the Auto-ID Centre at MIT, first mentioned the Internet of Things in a presentation he made to Procter & Gamble in 1999. Here's how Ashton explains the potential of the Internet of Things "Today computers -- and, therefore, the Internet -- are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code.

The problem is, people have limited time, attention and accuracy -- all of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things -- using data they gathered without any help from us -- we would be able to track and count everything and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling and whether they were fresh or past their best."

Humans could easily assign an IP address to every "thing" on the planet because of new Internet Protocol version 6 IPv6. According to Steve Leibson, with IPv6 address space expansion we could assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths. An increase in the number of smart nodes, as well as the amount of upstream data the nodes generate, is expected to raise new concerns about data privacy, data sovereignty and security.

Although the concept wasn't named until 1999, the Internet of Things has been in development for decades. The first Internet appliance, for example, was a Coke machine at Carnegie Melon University in the early 1980s. The programmers could connect to the machine over the Internet, check the status of the machine and determine whether or not there would be a cold drink awaiting them, should they decide to make the trip down to the machine.

THE HYPE CYCLE OF INTERNET OF THINGS (IOT)

According to Gartner, revenue generated from IoT products and services will exceed $300 billion in 2020, and that probably is just the tip of the iceberg. Given the massive amount of revenue and data that the IoT will generate, its impact will be felt across the entire big data universe, forcing companies to upgrade current tools and processes, and technology to evolve to accommodate this additional data volume and take advantage of the insights all this new data undoubtedly will deliver.

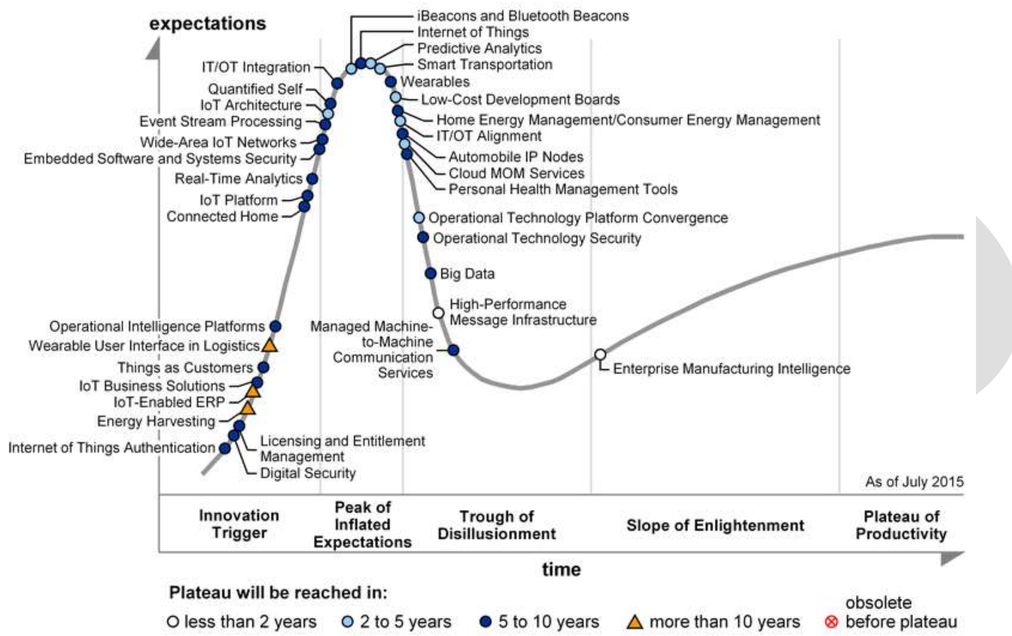

Figure 1. Hype Cycle for the Internet of Things, 2015

Organizations are connecting a broad variety of things to use their data to help build a digital business. Business objectives for IoT projects range from improved asset optimization to new business models, such as assets as a service. The IoT is a concept that is, in itself, transformational, and it will take five to 10 years to gain mainstream adoption. It remains on the Peak of Inflated Expectations again, as hype has continued to build even higher than last year — even as end users are not only building proof-of-concept projects, but encountering issues related to immature technologies, ecosystems and standards. Adoption of relevant IoT technologies and IoT-enabled business models varies on an industry-by-industry basis, so we have representative IoT technology profiles for specific markets (such as government, insurance and manufacturing operations) on the appropriate Hype Cycles.

Key building blocks for IoT projects include the following:

1. Have a Clear Objective
2. Connect to Your Things
3. Assemble and Integrate Your IoT Business Solution
4. Drive Value via Real Time Analytics

Some of the key near-term technology profiles for the IoT include:

- Big Data
- Embedded Software and Systems Security
- High-Performance Message Infrastructure
- IoT Architecture
- IoT Business Solutions

- IoT Platform
- IT/OT Alignment
- Low-Cost Development Boards
- Managed Machine-to-Machine Communication Services

KEY CHALLENGES

Like many evolving IT and networking technologies, the Internet of Things will encounter multiple barriers to adoption. Traditional inertia, budget priorities, risk aversion and other factors will prevent some companies from adopting IoT in the near future. Expect to see early adopters led by innovative CIOs or by business leaders identify and pursue specific opportunities to better serve their customers, open new businesses reduce costs and provide new value that results in increased revenues.

In addition to the technical challenges around power, latency, integration and storage, there are a number of other issues critical to IoT adoption. These challenges will also provide new business opportunities for technology companies, middleware and tools developers, system integrators, device builders and cross-platform integration companies. The main such key challenges are mentioned below:

1. Security: As the IoT connects more devices together, it provides more decentralized entry points for malware. Less expensive devices that are in physically compromised locales are more subject to tampering. More layers of software, integration middleware, APIs, machine-to-machine communication, etc. create more complexity and new security risks. Expect to see many different techniques and vendors addressing these issues with policy-driven approaches to security and provisioning.

2. Trust and Privacy: With remote sensors and monitoring a core use case for the IoT, there will be heightened sensitivity to controlling access and ownership of data. (Note that two recent high-profile security breaches at Target and Home Depot were both achieved by going through third-party vendors' stolen credentials to gain access to payment systems. Partner vetting will become ever more critical.) Compliance will continue to be a major issue in medical and assisted-living applications, which could have life and death ramifications. New compliance frameworks to address the IoT's unique issues will evolve. Social and political concerns in this area may also hinder IoT adoption.

3. Complexity, confusion and integration issues: With multiple platforms, numerous protocols and large numbers of APIs, IoT systems integration and testing will be a challenge to say the least. The confusion around evolving standards is almost sure to slow adoption. The rapid evolution of APIs will likely consume unanticipated development resources that will diminish project teams' abilities to add core new functionality. Slower adoption and unanticipated development resource requirements will likely slip schedules and slow time to revenues, which will require additional funding for IoT projects and longer "runways" for startups.

4. Evolving architectures, protocol wars and competing standards: With so many players involved with the IoT, there are bound to be ongoing turf wars as legacy companies seek to protect their proprietary systems advantages and open systems proponents try to set new standards. There may be multiple standards that evolve based on different requirements determined by device class, power requirements, capabilities and uses. This presents opportunities for platform vendors and open source advocates to contribute and influence future standards.

5. Concrete use cases and compelling value propositions: Lack of clear use cases or strong ROI examples will slow down adoption of the IoT. Although technical specifications, theoretical uses and future concepts may suffice for some early adopters, mainstream adoption of IoT will require well-grounded, customer-oriented communications and messaging around "what's in it for me." Detailed explanations of a specific device or technical details of a component won't cut it when buyers are looking for a "whole solution" or complete value-added service. IoT providers will have to explain the key benefits of their services or face the proverbial "so what."

6. High Level of required precision: "Both involve connecting devices and systems all across the globe, but the IoT add stricter requirements to its local networks for latency, determinism and bandwidth," the NI report notes. "When dealing with precision machines that can fail if timing is off by a millisecond, adhering to strict requirements become pivotal to the health and safety of the machine operators, the machines and the business."

Industry consortiums are working to address this challenge using standards originally developed for Audio/Video Bridging — the deceptively complex task of synchronizing video and audio in a stream.

7. Adaptability and Scalability: Adopting the Industrial Internet of Things will require a change in the way organizations design and augment their industrial systems. IoT systems must be adaptive and scalable through software or added functionality that integrates with the overall solution. As soon as an update is required, the engineer faces the dilemma of tacking on a solution that may not communicate well with the whole system or of starting the process over and creating a new end-to-end solution

INTERNET OF THINGS AND ITS IMPACT ON BIG DATA

The Internet of Things (IoT) is on its way to becoming the next technological revolution. Given the massive amount of revenue and data that the IoT will generate, its impact will be felt across the entire big data universe, forcing companies to upgrade current tools and processes, and technology to evolve to accommodate this additional data volume and take advantage of the insights all this new data undoubtedly will deliver.

A. Data Storage: One of the first things associated with IoT is a huge, continuous stream of data hitting companies' data storage. Data centers must be equipped to handle this additional load of heterogeneous data. In response to this direct impact on big data storage infrastructure, many organizations are moving toward the Platform as a Service (PaaS) model instead of keeping their own storage infrastructure, which would require continuous expansion to handle the load of big data. PaaS is a cloud-based, managed solution that provides scalability, flexibility, compliance, and a sophisticated architecture to store valuable IoT data. Cloud storage options include private, public, and hybrid models. If companies have sensitive data or data that is subject to regulatory compliance requirements that require heightened security, a private cloud model might be the best fit. Otherwise, a public or hybrid model can be chosen as storage for IoT data.

B. Big Data Technologies: When selecting the technology stack for big data processing, the tremendous influx of data that the IoT will deliver must be kept in mind. Organizations will have to adapt technologies to map with IoT data. Network, disk, and compute power all will be impacted and should be planned to take care of this new type of data. From a technology perspective, the most important thing is to receive events from IoT-connected devices. The devices can be connected to the network using Wi-Fi, Bluetooth, or another technology, but must be able to send messages to a broker using some well-defined protocol. One of the most popular and widely used protocols is Message Queue Telemetry Transport (MQTT). Mosquitto is a popular open-source MQTT broker. Moreover, for IoT data, NoSQL document databases like Apache CouchDB are more suitable as they offer high throughput and very low latency. These types of databases are schema-less, which supports the flexibility to add new event types easily. Other popular IoT tools are Apache Kafka for intermediate message brokering and Apache Storm for real-time stream processing.

C. Data Security: The types of devices that make up the IoT and the data they generate will vary in nature - raw devices, varied types of data, and communication protocol – and this carries inherent data security risks. This heterogeneous IoT world is new to security professionals, and that lack of experience increases security risks. Any attack could threaten more than just the data – it also could damage the connected devices themselves. IoT data will require organizations to make some fundamental changes to their security landscape. As the IoT evolves, an unmanaged number of IoT devices will be connected to the network. These devices will be of different shapes and sizes and located outside the network, capable of communicating with corporate applications. Therefore, each device should have a non-repudiable identification for authentication purposes. Enterprises should be able to get all the details about these connected devices and store them for audit purposes. All internal and external core routers/switches should be instrumented with X.509 certificates for creating trusted connectivity between public and private networks. A multi-layered security system and proper network segmentation will help prevent attacks and keep them from spreading to other parts of the network. A properly configured IoT system should follow fine-grained network access control policies to check which IoT devices are allowed to connect. Software-defined networking (SDN) technologies, in combination with network identity and access policies, should be used to create dynamic network segmentation. SDN-based network segmentation also should be used for point-to-point and point-to-multipoint encryption based on some SDN/PKI amalgamation.

D. Big Data Analytics: IoT and big data basically are two sides of the same coin. Managing and extracting value from IoT data is the biggest challenge that companies face. Organizations should set up a proper analytics platform/infrastructure to analyze the IoT data. And they should remember that not all IoT data is important. A proper analytics platform should be based on three parameters: performance, right-size infrastructure, and future growth. For performance, a bare-metal server, a single-tenant physical server dedicated to a single customer, is the best fit. For infrastructure and future growth, hybrid is the best approach. Hybrid deployments, which consist of cloud, managed hosting, colocation, and dedicated hosting, combine the best features from multiple platforms into a single optimal environment. Managed Service Providers (MSPs) are also working on their platforms to handle IoT data. MSP vendors are typically working on the infrastructure, performance, and tools side to cover the entire IoT domain.

An IoT device generates continuous streams of data in a scalable way, and companies must handle the high volume of stream data and perform actions on that data. The actions can be event correlation, metric calculation, statistics preparation, and analytics. In a normal big data scenario, the data is not always stream data, and the actions are different. Building an analytics solution to manage the scale of IoT data should be done with these differences in mind.

The growth of the IoT heralds a new age of technology, and organizations that wish to participate in this new era will have to change the way they do things to accommodate new data types and data sources. And these changes likely are just the beginning. As the IoT grows and businesses grow with IoT, they will have many more challenges to solve.

CONCLUSION

The Internet of Things is a new wave of technology advancement in the early stages of market development. Like many preceding waves of technology evolution it is characterized by innovation, fragmentation, confusion, competitive jostling and emerging standards. Startups are shaking up the status quo as established technology companies react and adjust.

The IoT will leverage, embrace, extend and enhance cloud, big data, personal/mobile devices and social networks to provide more granular sensors and devices closer to the “edge.” As it does so, it will provide entirely new applications and use cases that will drive new business models and revenue opportunities. It will also threaten many existing industries, markets and products.

It will likely collide and impact adjacent disrupting trends and markets. For example, the IoT has the potential to further accelerate the “sharing economy.” By providing new ways to track and manage smaller things, it will enable the sharing of new, smaller and less expensive items beyond houses, planes, cars and bikes. In some ways the IoT is the next logical extension of the “long tail” concept. It pushes devices and sensors to more granular levels and enables the creation of new uses, new applications, new services and new business models that were not previously economically viable.

As the IoT evolves, much of the value will migrate from devices and components into “whole solutions” and services. Therein lie the opportunities for new value creation, new business models and new revenue streams for market participants. A bigger challenge than developing technology breakthroughs may be in answering the question “What problems can be solved with the IoT and what new value can be provided to customers?”

REFERENCES:

[14] The Internet of Things: A survey by Luigi Atzoria, , Antonio Ierab, , Giacomo Morabit

[2] Internet of Things (IoT): A vision, architectural elements, and future directions by Jayavardhana Gubbia, Rajkumar Buyya, Slaven Marusica, Marimuthu Palaniswamia

[3] Smart objects as building blocks for the Internet of things by Gerd Kortuem ; University of Lancaster, ; Fahim Kawsar ; Vasughi Sundramoorthy ; Daniel Fitton

[4] The Internet of things in the cloud: A Middleware perspective, Honbo Zhou 2012 ,CRC Press.

[5] The Internet of Things – Key applications and Protocols, Olivier Hersent, David Boswarthik, Omar Elloumi, 2012, Wiley.

[6] Architecting the internet of things, Dieter Uckelmann, Mark Harrison, Florian Michahelles, 2011, Springer.

[7] http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[8] https://en.wikipedia.org/wiki/Internet_of_things

[9] http://sandhill.com/article/the-internet-of-things-challenges-and-opportunities/

[10] http://www.cio.com/article/2872574/it-industry/5-key-challenges-facing-the-industrial-internet-of-things.html

[11] https://www.gartner.com/doc/reprints?id=1-2M904VI&ct=150901&st=sb

[12] http://data-informed.com/the-impact-of-internet-of-things-on-big-data