IoT Market Landscape
June 19, 2016

M. R. Pamidi, Ph. D.
Editor-in-Chief
IT Newswire

Executive Summary

The Internet of Things (IoT) market is on a roll and some expect this to show exponential growth in the next decade. Skeptics see too much marketing hype and another *déjà vu* all over again, with a tech bubble on the horizon. We see neither, but expect an initial moderate growth with a slight market correction (where many of the hype-heavy vendors will vanish), followed by market consolidation, and steady growth thereafter.

1. Introduction

IoT has been gaining a lot of momentum over the past few years and what was once hype is now morphing into a money-making machine. With an expected 50 billion devices by 2020[1] and a forecasted US$11.1 trillion per year in 2025[2] for IoT applications, everyone is jumping onto the IoT bandwagon (Figure 1).
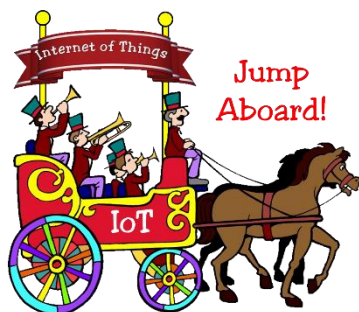

While some vendors are still stuck in the marketing-hype era, others are rolling out real-world products adding value to their traditional businesses. IoT is nothing new, it has been called *machine-to-machine* in the past and been in use in industrial control systems and the manufacturing floor for decades. Consumer goods manufacturers and retailers have long used RFID tags on shipping pallets to manage inventory. Lately, other industries have discovered it and a plethora of vertical industry-specific solutions is emerging. The IoT landscape (Figure 2) is very crowded, with hundreds of vendors covering every aspect of life one can imagine.
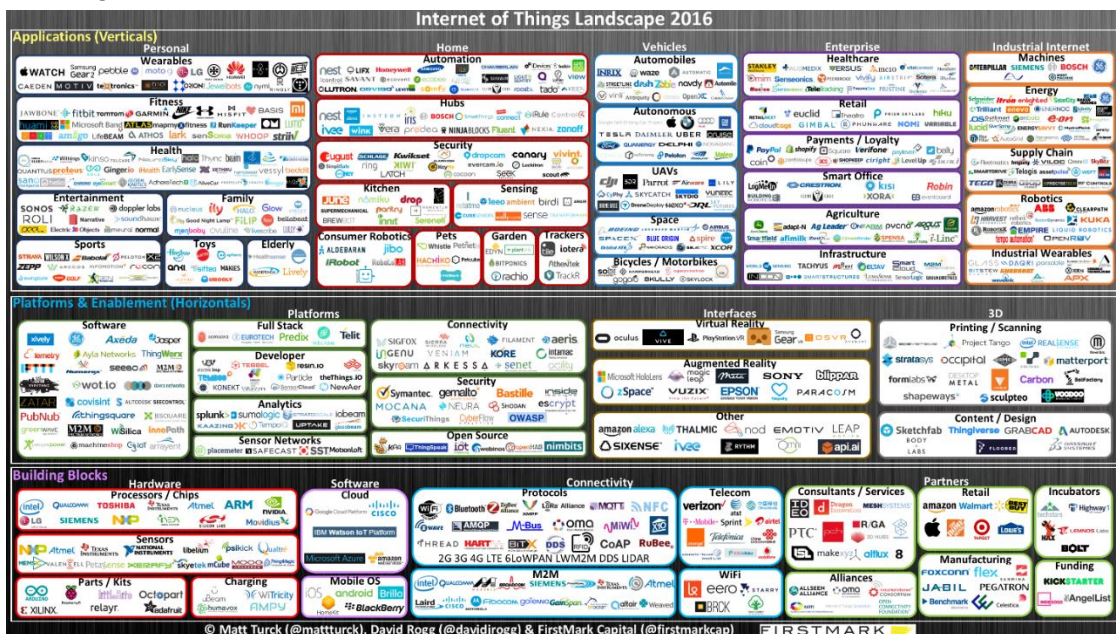
Figure 1. IoT Bandwagon

Figure 2. IoT Landscape

[1] "Internet of Things in Logistics," DHL Trend Research and Cisco Consulting Services, 2015.
[2] "Unlocking the potential of the Internet of Things," McKinsey, June 2015.

2. IoT Market Drivers

While the common drivers for adopting IoT among all industries are reducing human errors and enhancing machine-to-machine communications, there are certain industry-specific characteristics that are influencing organizations to invest in IoT. We discuss below five industries where IoT is changing the very way business is done.

2.1 Manufacturing

There are concerns about America's declining manufacturing prowess by handing it over to China and other countries with low labor costs. We believe this industry, driven by IoT and increasing automation, will come roaring back with a vengeance and the U. S. becoming the envy of the world.

The following drivers will encourage and reinvigorate investments in IoT.

- **Predictive maintenance and operations management** can result in savings of between US$1.2 trillion and US$3.7 billion by 2025, according to McKinsey.[3]
- **Emerging-markets growth:** While the PIIGS (Portugal, Ireland, Italy, Greece, Spain) countries are still recovering financially and four of the five BRICS (Brazil, Russia, India, China, South Africa) countries are facing challenging times, manufacturers continue to look for other emerging markets for growth.
- **RFID and Sensors**: Sensor data that are used to predict when equipment is wearing down or needs repair can reduce maintenance costs by as much as 40 percent and cut unplanned downtime in half. EPCglobal, the standards body for the RFID industry, has set a goal to reduce the cost of an RFID tag, now 15 cents, to five cents and make them practical for tracking low-value inventory in manufacturing, retail, and shipping.
- **Shortage of expertise**: An aging workforce with workers with a significant amount of expertise at or reaching retirement age and declining numbers of new graduates in manufacturing- and engineering-related disciplines. Exceptions are countries like Germany and The Netherlands where institutions like Technische Hochschule (now called Technische Universität) train engineers in specialty areas to meet industry needs when they graduate.
- **Traceability, transparency, and brand reputation:** Manufacturers will use increased traceability and transparency to strengthen their ability to deliver product quality and protect their reputations. One example is the mandate to report the use of conflict minerals—tantalum, tin, tungsten, and gold—in their products, as required by Section 1502 of the Dodd-Frank Act of 2010.[4]
- **Ubiquitous connectivity.** Connectivity in devices, interfaces, and processes is ubiquitous and extends to the edge, with manufacturers assuming that the communication infrastructure will keep up.

2.2 Healthcare

Healthcare industry in the U. S. is transforming radically for a variety of reasons:

- Controlling the ever-increasing costs of providing care, prescription medicines, and medical devices.
- Meeting Affordable Care Act mandates, especially implementing EHR/EMR systems—a challenge to the industry used to faxes, dictation machines, and rows and rows of shelves loaded with medical records, X-Rays, CT and MRI scans stored in hospital basements or in warehouses miles away from hospitals.
- Tracking expensive medical equipment—CT and MRI Scanners and X-Ray machines—in large hospitals and avoiding investing in additional, redundant equipment.

Embedded systems, *inter alia*, play a major role throughout IoT-driven healthcare systems, including, but not limited to:

- Sensors that collect patient data
- Microcontrollers that process, analyze, and wirelessly communicate the data
- Microprocessors that enable rich graphical user interfaces
- Healthcare-specific gateways through which sensor data is further analyzed and sent to the cloud

---

[3] "Unlocking the potential of the Internet of Things," McKinsey, June 2015.
[4] "FACT SHEET: Disclosing the Use of Conflict Minerals," US SEC, July 29, 2014.

One of the most fascinating and challenging applications of IoT is caring for per-mature babies ("preemies") in neonatal/pediatric intensive-care units (N/PICUs). Preemies lack red blood cells to carry oxygen to their tissues and need to be on oxygen respirators with the right amount of oxygen flow rate—insufficient amounts result in death and excessive amounts result in blindness. So, the oxygen supply has to be optimal and a baby's condition is constantly monitored and sent wirelessly to the N/PICU nurse on duty.

2.3 Mining and Metals

IoT contributes to ground-breaking changes for the mining and metals industry segments. These highly complex industries navigate remote and often hazardous global operations, far-flung supply chains, and the turmoil of price and demand volatility. Thriving companies strive to continuously adapt and try new business and technology approaches to innovate and achieve efficiencies that support profitability as well as a commitment to sustainability and responsible mining.

The top priorities for building a successful IoT strategy are:

- ***Connected Asset Management Connected Operations***: Forward-looking and cost-conscious companies know asset uptime and failure prevention are crucial. Companies can perform maintenance before problems arise, using machine sensors to monitor real-time environmental and performance indicators. GE, Hitachi, Rio Tinto, and Siemens are doing pioneering work in this area.
- ***Connected Logistics – Vehicle Management and Tracking***: A well-known international steel company uses IoT to bring its entire 3,700-vehicle fleet management process online. GPS and RFID systems are used to monitor equipment movement, fuel levels and consumption, and all associated transactions. Annually, the company is saving 5% on maintenance and 10% on fuel costs.
- ***Connected Operations – Real-Time Production and Delivery***: Another multinational steel company is improving its business process management with a new integrated operations center driven by IoT. On a large video wall, real-time information enriched with visual key performance indicators gives operators information for the integrated management of production and delivery. GPS tracking of material movements, as well as camera views of production, further improve the planners' decisions. The video wall provides all production information, including materials, logistics, schedules, and energy, across the plant supply chain.
- ***Remote Service Management – Predictive Maintenance***: A global equipment manufacturer is revolutionizing the maintenance of its machines and equipment using alerts captured with telematics technology combined with warranty claims information. This provides visibility into massive amounts of new data and the ability to recognize issues two to three months faster than before.

2.4 Food Distribution

In developing countries food *storage* and *distribution* are more crucial than food *production*. Every year 1.3 billion tons of food valued at US$1 trillion are lost due to spoilage. Reducing waste by 25% would feed 850 million people. RFID technology at every stage of the food chain—warehouses, transportation, distribution, and storage at retail warehouses and stores—could reduce spoilage and alleviate this problem.

2.5 Smart Buildings, Homes, and Cities

Smart Buildings

Many modern buildings have motion sensors to control lighting, but what is emerging is highly granular motion-controlled HVAC systems, so that the air conditioning or heating turns off when there are no occupants in an area. Additionally, traditional systems were standalone, but now are on IP networks, so the entire HVAC system is controlled by IT. Thus, IT is no longer a *cost center*, but is a *cost-control center*. Figure 2 shows what a smart building could look like.

Similar technologies are also being deployed in restrooms in buildings where connected paper towel and bathroom tissue dispensers are instrumented and when they are running low, notify the building maintenance staff who otherwise would routinely make unnecessary rounds. This is akin to soft drinks and snacks vending machines notifying local warehouses when they are running low on supplies.
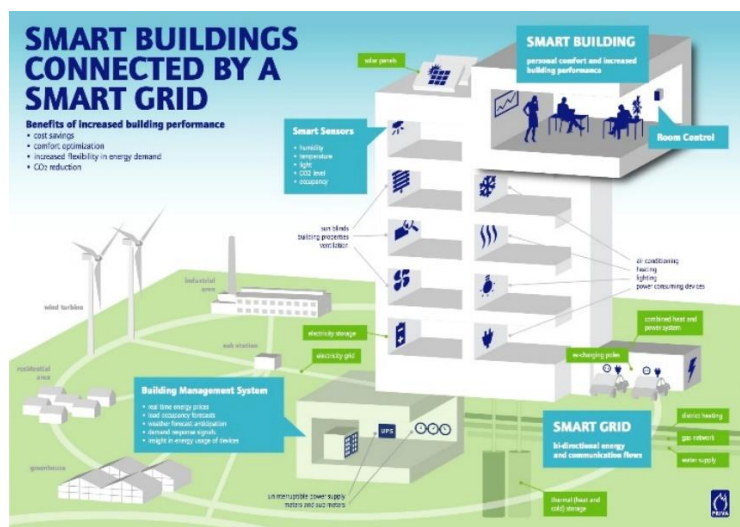
Figure 2. Smart Building of the Future

Smart Homes

The smart home market is set to grow in the next five years from $43 billion in worldwide revenue in 2015 to more than $100 billion by 2020, according to Juniper Research.[5] A 'Smart Home" (Figure 3) is supposedly where every device in your home is wirelessly 'connected' and they all can talk to one another through Bluetooth, Bluetooth Low Energy, Wi-Fi, ZigBee, Z-Wave, or any of the other established or emerging industry protocols.
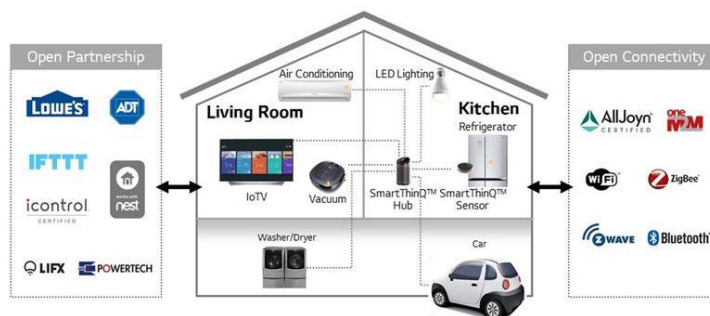

Figure 3. Smart Home

These all look great on paper with nice graphics, but the smart devices depicted here are not cheap and still not within the reach of the average consumer. You can buy a brand name stainless steel fridge for a little over US$1,000. Why would you want to pay almost US$7,000 for a Wi-Fi-enabled 'smart' fridge with a screen and keeps nagging you "I'm out of milk, bread, and eggs, buy some?" Your spouse does it for you for free! Also, the recent hacking of Samsung's SmartThings and last year's attack on a Samsung smart fridge that let hackers steal Gmail credentials have left customers confused about the whole idea of smart homes with dumb devices. True, the vendors are all excited about the revenue potential here, but unless the prices of these appliances come down drastically, which we believe in the next five years, and security concerns are fully addressed, consumers will be reluctant to become prey of vendors' marketing hype.

---

[5] "Why Samsung's SmartThings Home Controller Is Under Fire," Don Reisinger, *eWeek*, May 3, 2016.

Smart Cities

A smart city (Figure 4) is an urban development vision to integrate multiple information and communication technology (ICT) solutions in a secure fashion to manage a city's assets — local departments, information systems, schools, libraries, transportation systems, hospitals, power plants, water supply networks, waste management, law enforcement, and other community services.[6]

Figure 4. Smart City

Cities around the world are spending billions of dollars modernizing their cities' infrastructure—parking, traffic lights, street lighting, water supply systems, and garbage collection and recycling, to mention a few. In many cases, there are huge payoffs and in other cases, a bit of skepticism.

The City of Palo Alto, CA, under the leadership of a visionary CIO, has done some very interesting work and deployed Smart Traffic Infrastructure to analyze traffic patterns and parking availability. The work is so impressive that the City of Boston contacted Palo Alto for help. It snows in Boston in winter (that's an understatement) and under very heavy snowfall the fire hydrants in the city neighborhoods get buried in many feet of snow. So, when the Boston Fire Department arrives to put out a fire, they can't locate fire hydrants. After discussions with the City of Palo Alto, Boston is installing beacons on fire hydrants and the citizens of Boston have 'adopted' (think of Adopt-A-Highway) their neighborhood hydrants and clear the snow around them so the Fire Department can do a more effective job.

Chicago is building a permanent infrastructure to collect Big Data. The city is installing hundreds of environmental sensors to measure temperature, humidity, light, sound, and cellphone signals. All this data is supposed to enable Chicago to become a safer and cleaner city. The sensors will be placed on top of lampposts along Chicago's Michigan Avenue. Skeptics argue this is just a step to enrich tech vendors, with questionable ROI. We would also add one of Chicago's major problems is homicide and the city faces a 62 percent increase in homicides. Through mid-May, 216 people have been killed (Figure 5) and shootings are up 60 percent. One Chicagoan we talked to at a recent IoT conference lamented "Our big problem is rodents, not roads."
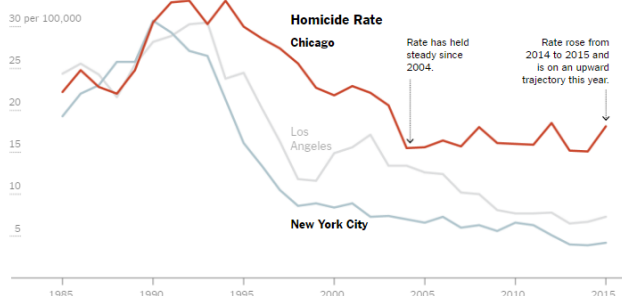

Figure 5. Chicago Homicide Rate[7]

---

[6] Wikipedia
[7] "Chicago's Murder Problem," Ford Fessenden and Haeyoun Park, *The New York Times*, May 27, 2016.

Will Smart City work in Detroit that has more serious problems of high unemployment and population loss? Unless there is a compelling ROI, cities will be reluctant to technologies that don't deliver immediate benefits with social impact. Many small cities may not even have the IT staff to manage all the smart devices. In these cases, we expect Service Providers, and not the technology vendors, will play a major role in deploying and maintaining the IoT infrastructure.

3. What should be your strategy?

An IoT strategy should be established not to just jump into the IoT ocean like lemmings and drown in tech gobbledygook, but swim in the IoT stream only if it truly adds value to your business. IoT is an innovation accelerator, but how does it change your business model?

To establish an IoT strategy:
1. Assign a central IoT team that includes IT and various lines of businesses.
2. Identify what solutions fit in your IoT context.
3. Kickstart a project, identify which processes can be improved with IoT, and develop a proof of concept.
4. Adopt any standards relevant to your project.
5. Don't be shy to confer with your competitors to learn from their experiences.
6. Establish realistic metrics and periodically measure your progress against them.

4. IoT Monetization

Forward-looking and innovative organizations are moving beyond the IoT hype and generating revenues. We can quote scores of examples, below are some interesting ones where innovation is removing friction:

- Commercial buildings consume 47 percent of global energy, about half of that coming from chillers. Keeping on top of chiller performance is critical, not just for efficiency, but for occupant comfort and productivity. New IoT technologies developed by Johnson Controls are making it easier to stay on top of chiller maintenance – with data available anywhere, remote monitoring and diagnostics allow service technicians to proactively tackle potential issues, making preventive care and maintenance scheduling easier than ever.
- Aquacloud provides a cloud-based monitoring platform for commercial aquaculture and municipalities. It doesn't sell, but rents, a system that currently provides real-time readings of temperature, pH, dissolved oxygen, and conductivity in water. Listening to customers' requests, the company will be adding more sensors in the near future including: nitrate, nitrite, ammonia, depth, chlorophyll, turbidity, and blue-green algae.
- Airbnb, Lyft (does over 7 million rides a month), and Uber (fulfills one million rides daily) are basically using IoT to connect consumers and suppliers and generating revenues.

5. IoT Privacy and Security

Tons of discussions, research articles, and papers have been published on these very important topics. We'll summarize some comments from speakers and attendees we interviewed at two recent conferences that we attended: IoT World and IoT Developers Conference.

- Security costs money.
- Security in IoT is difficult because IoT uses so much open source that constantly changes.
- In IoT there are multiple sources and types of data with questionable or unknown pedigree.
- We *could* try stateless key management for structured date and identity-based encryption for unstructured data.
- Security is required in both the data and the device. For instance, you decide to have a spaghetti dinner tomorrow and, to save time, leave a pot of water on your Wi-Fi-enabled smart gas range in your home and program it from your smartphone to turn the range on five minutes before you come home. But a hacker infiltrates your home Wi-Fi network, turns the gas line on, but deactivates the gas range. You come and, unable to smell the gas, light the gas range. BOOM!
- The Internet is the least regulated industry; how can we bring discipline here?
- Can we think of star ratings for security, as we have ENERGY STAR for appliances? If we do, who assigns them?

6. Conclusions

The IoT landscape is constantly changing, new players are constantly appearing in the landscape, many small players are being gobbled up by the larger fish, and some hype-heavy, content-free vendors are biting the dust. The landscape two years out may not be what it looks like today. The IoT Gold Rush, similar to the Dot-Com boom is on and who will make the money—the gold diggers or the shovel, jeans, and implements makers—is yet to be seen. Stay tuned.