The Internet of Things (IoT):

Strategic IT in the Age of Digital Disruption

Case Analysis

By: Team 9

Ashwin Gayash, Xiaowei Fan, Jae Kyung, Matt Urquhart

Loosely defined, the Internet of Things is about creating an intelligent network of smart devices - devices such as embedded circuits, smart phones, sensors, software, etc. - to create efficiencies, automation, quality of life improvement, economic benefits, and more. In many cases, IoT information infrastructure relies upon internet connectivity, but IoT benefits can be realized over local networks as well - the key is about creating more direct integration of physical devices and benefitting from a more intelligent system as a result. IoT is comprised of three types of components: hardware, middleware, and presentation. Hardware is easiest to imagine - this layer is commonly the existing embedded device, such as sensors, actuators, or communication devices. Middleware can be thought of as the glue that transmits data to and from hardware devices, stores data, and analysis of data from the system as a whole. Finally, presentation describes the software layer that end users can use to consume the data in a more meaningful way, through data visualization or reporting for example[1].

Interestingly, IoT is not really a new concept, but rather builds on existing machine-to-machine communications concepts, or M2M, that has been around for decades[2]. However, IoT goes beyond M2M. In order to be defined as an IoT system, the system must go further than simply networking devices together for communications. IoT systems are in essence more than a sum of their parts. Not only do they function and communicate with one another in a single ecosystem, they feed off of analysis from its various data sources to provide smart-functionality that would otherwise not be possible. Furthermore, in the context of internetworking, IoT architecture and platforms must be built so that all subcomponents are linked together including analytics, data, an integration layer, aggregated device management, gateways, and the user interface.

IoT has become big business in the 2010s in part due to the rise of a combination of technologies that make possible the kinds of M2M communications and analytics that were not available before. Now we have things like factory sensors and home appliances that have embedded chips for computing and network connectivity, we have smart phones, we have available compute to do big data analysis and machine learning on large quantities of data from such subsystems - all of which today are frequently used in IoT systems and yet would not be practical or even feasible just a few years ago. Businesses today are rapidly researching ways to leverage this new capability in ways that activates their IT strategies, to provide practical IoT applications that enable users to operate more efficiently or automate previously manual tasks in their networks.

In Gartner's IT Hype Cycle (2015), IoT is an emerging technology, and it is estimated that IoT will be adopted by the market at a considerable scale in next 5 to 10 years[3]. It is essentially at the peak of its hype cycle, largely due to what businesses see as limitless opportunities to implement this technology to activate IT strategy and realize real competitive advantage. So how is IoT being implemented?

An easily understood category of IoT solutions for everyday use is that of home automation. Think of the Nest thermostat[8], which is designed to save money for customers by giving them the ability to regulate their home temperature from their smartphone. It is programmable so that at times nobody is at home, climate control is limited or disabled. When it gets close to time for somebody to come home, it will gradually heat or cool until the home is a comfortable temperature by the time the customer gets home. And at any time, you can monitor home temperature or make adjustments via your smart phone. Nest, owned by Google's parent company, Alphabet, is a leading innovator in IoT home automation. They also offer similar solutions for home security cameras, smoke alarms, and are working on integration with Google home - a voice activated system that allows the user to tell Google home what commands to give to other devices within their home IoT. Other examples of home automation leveraging IoT systems are internet-capable washer and dryers, or refrigerators. Samsung has a fridge that will let you check if your food is going to spoil soon from your phone[9]. It's not a stretch to imagine that with internet connectivity and a digital shopping list, an IoT fridge could check on when food will spoil, and pre-emptively order new food items from a service such as Amazon Prime Pantry automatically as a replacement. Certainly a technology disruption for grocery stores and outlets nationwide.

The medical field is already looking to capitalize on the automated fridge concept in order to ensure that vaccines worldwide are managed effectively[7]. According to the World Health Organization, roughly 1.5 million children die each year from vaccine-preventable diseases. With this Bluemetal IoT capable vaccine refrigerator technology, coupled with Microsofts IoT Machine Learning hub, vaccines can be both protected throughout the supply chain and doctors can ensure that vaccines do not experience shortages where they are needed the most.

In an example more relevant to manufacturing industries, our own team member, Matt Urquhart is the lead security architect for an IoT project currently under way at The Hershey Company. In this example, Hershey is aiming to pilot a Twizzlers production line in an effort to improve the lines efficiency. If successful, the same concept can be expanded to its more lucrative chocolate lines. The concept is to integrate the line equipment - specifically the extruder (which is a device that is designed to cut product into a fixed segment) and net weight machines - with Microsoft's Azure IoT Machine Learning hub[6]. By constantly measuring line performance, line equipment configuration, temperature and product weight, the Azure IoT hub - through machine learning - can make suggestions to line configuration that translates to less product wasted by the extruder. At Hershey, the licorice lines are already estimated to be highly efficient, but if the pilot can succeed and be implemented on chocolate lines, cutting down extruder waste on chocolate could translate to tens of millions of dollars for the company. A successful implementation will translate directly to an example of a unification IT architectural

implementation - a single business unit with global data access and similar business processes across chocolate and licorice. Improving line efficiency through IoT will drive key process improvement and activation of company strategy via IT advantage for Hershey. This is a perfect example of how IT strategy can directly drive business strategy and competitive advantage.

With all of the potential of IoT, there are some key challenges to overcome. A large challenge is privacy and security, which is alluded to by virtue of the previous Hershey example needing a security architect to help with the design and implementation. In every example mentioned thus far, at least some of the data required to make the IoT system itself work is sensitive - data that, communicated over any network, let alone the internet, should be secured from potential attackers who may be sharing the network.

Take home automation for example. In the Nest example if we take the thermostat, or the security cameras - in order for the end user to control these devices on their mobile device, there needs to be a web service layer exposed to the internet from the home network which those devices are on. For anyone security savvy, that should already be a red-flag. If compromised, a potential attacker may be able to take control of the security cameras and make it easier to rob your house. Any customer should seek assurance that security preventing such a scenario is in place, otherwise the purpose of having security cameras is defeated in the first place.

Generally, privacy and security can be solved using techniques such as network segmentation and data encryption. Segmentation is a straightforward concept - isolate networks and traffic going to the internet from networks with sensitive data to mitigate risk in a compromise scenario. For the home user in the Nest example, perhaps this means that your Nest appliances are not on the same network as your home computer, for example, so that an attacker who theoretically compromises the Nest web services has no network route to other home devices. In the Hershey example, or other corporate scenarios, it usually involves expensive next-gen firewalls to isolate SCADA (manufacturing) equipment from direct internet connectivity or other subnets of the corporate network.

Encryption is a more preventative measure. Using TLS or SSL with Public Key Infrastructure (PKI), individual IoT devices can be authenticated to one another using certificates, such as an X509 certificate. At Hershey for the Twizzlers example, not only is all internet traffic to and from the Azure cloud IoT hub encrypted via TLS, each individual device will be authenticated, so TLS will be used to encrypt data transmitted in such a way that only authorized devices in the IoT system will be able to decrypt the data. For Hershey, the security component is critical because if compromised, the IoT system has control over the production line. In such a scenario, a potential attacker could take the line down costing the company millions of dollars. Even though there are options to secure the implementation, they tend to be costly, and risk is high.

In order to overcome these challenges and grow IoT solutions, IT departments must find cost efficient ways to address security concerns and the potential for solutions to scale. Cloud computing platforms will drive growth in this area because they have the compute capacity to scale machine learning and big data aspects of IoT solutions. Another driver of growth of IoT solutions will be the improvement of networking infrastructure - as cellular and traditional networks increase bandwidth, and as more and more devices become internet-aware, the applications for IoT solutions will become greater, both over wider area networks and incorporating a wider variety of embedded systems.

Overall we have demonstrated that it is fairly clear that IoT has tremendous potential in a variety of different use cases. However, which stakeholders stand to gain or lose as a result of this disruptive technology? In short, it really depends. Manufacturing companies who manage to successfully become early adopters, such as potentially Hershey, can create a competitive advantage in making a more efficient production process. However, in the specific example of manufacturing, line efficiency improvement over the long term is so imperative to the business that, if successful, IoT will be more of a requirement just to produce - meaning that early adopters like Hershey may experience a short term advantage, but very obvious efficiency gains coupled with a relatively easy cloud-based implementation will mean that competitors catch up fairly quickly.

The real benefactors of IoT will be end customers, entrepreneurs like Nest who design innovative new IoT solutions benefitting customers in a blue ocean strategy, and cloud vendors like Microsoft who can offer cloud-based, highly scalable IoT and Machine Learning solutions to companies to improve their own operational efficiency. Things like home automation aim to substantially simplify people's lives, which will translate to more leisure hours in the day. In the example of the vaccine fridge, millions of lives can be saved.

Conversely, automation gains through IoT may make some services obsolete. Take the automated home refrigerator example. Conventional brick-and-mortar grocery stores could genuinely be at risk of losing business due to such a technology - who likes going to the grocery store shopping if your fridge can do all the work for you?

In conclusion, we have demonstrated through several examples how IoT technology can be used to integrate existing technical solutions into interconnected ecosystems that can drive sustained efficiency improvements to key business processes. Despite challenges for early adopters, as standards and protocols for IoT communication become more streamlined, and as compute and memory becomes more readily available, solving for scalability and security issues will become more and more cost effective. And finally, in every example we demonstrate clear alignment of IT strategy with business strategy activation. IoT is sure to be an innovation to stay for some time.

References

1. Gubbi et al., 2013
2. An example of M2M: A vending machine can message the distributor when a particular item is running low to signal a need for restocking. knowledge.wharton.upenn.edu/article/leveraging-the-internet-of-things-for-competitive-advantage/ These things vary from physical objects, such as sensor, to virtual entities that communicate big data dynamically to enhance operational efficiency and even change value propositions for many businesses.
3. Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor Devices are smart because some electronics are embedded to enable seamlessly sensing, computing, communications, and data transfer in the IoT network.
4. Westerman, G. (2014) The Internet-Connected Engine Will Change Trucking hbr.org/2014/11/the-internet-connected-engine-will-change-trucking/
5. Lee, I. and Lee, K. (2015) 'The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises', Business Horizons, 58(4), 431-440. sciencedirect.com.ezproxy.lancs.ac.uk/science/article/pii/S0007681315000373
6. "Azure IoT Suite | Microsoft Azure." *Azure IoT Suite | Microsoft Azure*. N.p., n.d. Web. 17 Oct. 2016. https://azure.microsoft.com/en-us/suites/iot-suite/.
7. Barb Edson - General Manager, Marketing, Cloud and Enterprise. "IoT-enabled Smart Fridge Helps Manage Vaccines and Saves Lives." *Internet of Things*. N.p., 16 Aug. 2016. Web. 17 Oct. 2016. https://blogs.microsoft.com/iot/2016/08/16/iot-enabled-smart-fridge-helps-manage-vaccines-and-saves-lives/.
8. "Meet the Nest Learning Thermostat." *Nest*. Nest Labs, Inc., n.d. Web. 17 Oct. 2016. https://nest.com/thermostat/meet-nest-thermostat/.
9. "Samsung's Fridge of the Future Will Let You Check Spoilage from Your Phone." *The Verge*. N.p., 04 Jan. 2016. Web. 17 Oct. 2016. http://www.theverge.com/2016/1/4/10707894/samsung-smart-refrigerator-connected-fridge-iot-ces-2016.

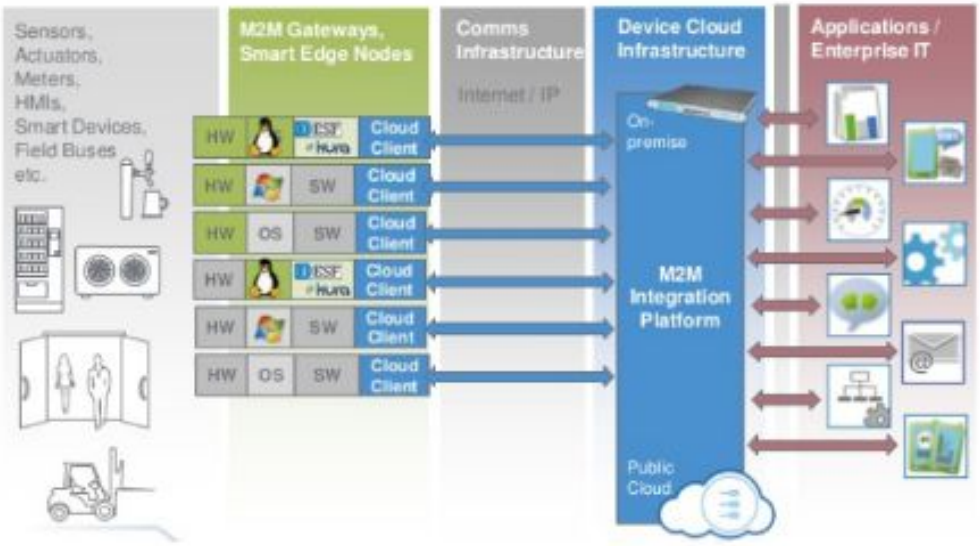
Appendix

Additional applications offering competitive advantage can be categorized into 3 groups of usage:

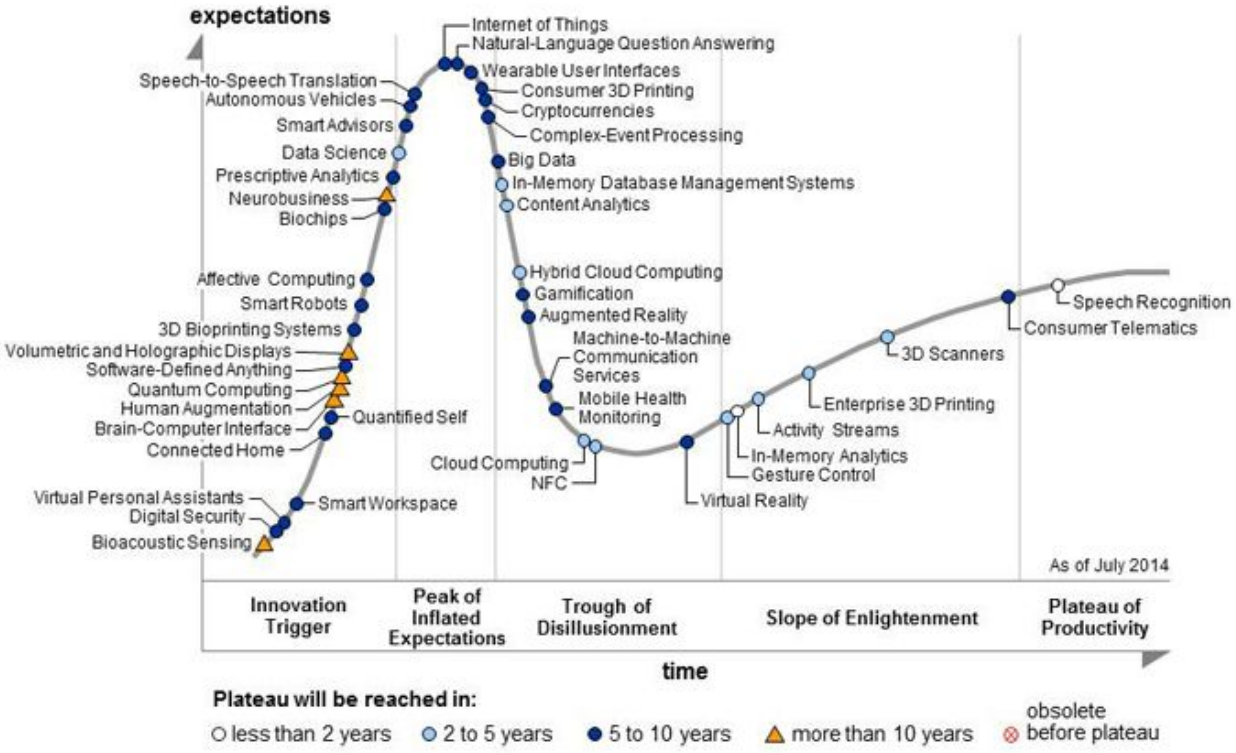
- information sharing and collaboration (for marketing and after service)
- monitoring (for operations maintenance)
- data analytics (for improved customer experience)

With information sharing and collaboration, location-based service apps use the IoT to market their products and services, and also improve user experiences. To illustrate, smart, connected products that can communicate with consumers' home ecosystems to accept inputs like weather and transmit the data to the business to discern the product use patterns and better understand their customer needs. Such functionality will enable manufacturers to closely monitor product performance and allow new service offerings that, for example, help the user avoid an overload when the washing machine is connected to other gadgets in the home or shift electrical costs and optimize energy consumption. Also, through real-time updates and quality control, predictive maintenance can be performed on the fly, with the app being used to alert the aircraft operator to a critical issue - If any part of the engine needs to be replaced it will be directly ordered and shipped, bypassing the order process and saving time.[4] Thirdly, with big data and data analytic capabilities, IoT can be used to collect, aggregate and analyze data for business insights to help businesses and consumers make better decisions. For instance, health care companies can provide customized services to heart patients by pulling in data from wearable sensors to its platform and combining the biometric and medical record data to offer innovations such as "smart pill bottles" that track whether or not they've taken their medication, and perform predictive analytics to identify which patients are least likely to stick to drug therapy regimens and thus need more intervention from caregivers to significantly improve outcomes.[5]

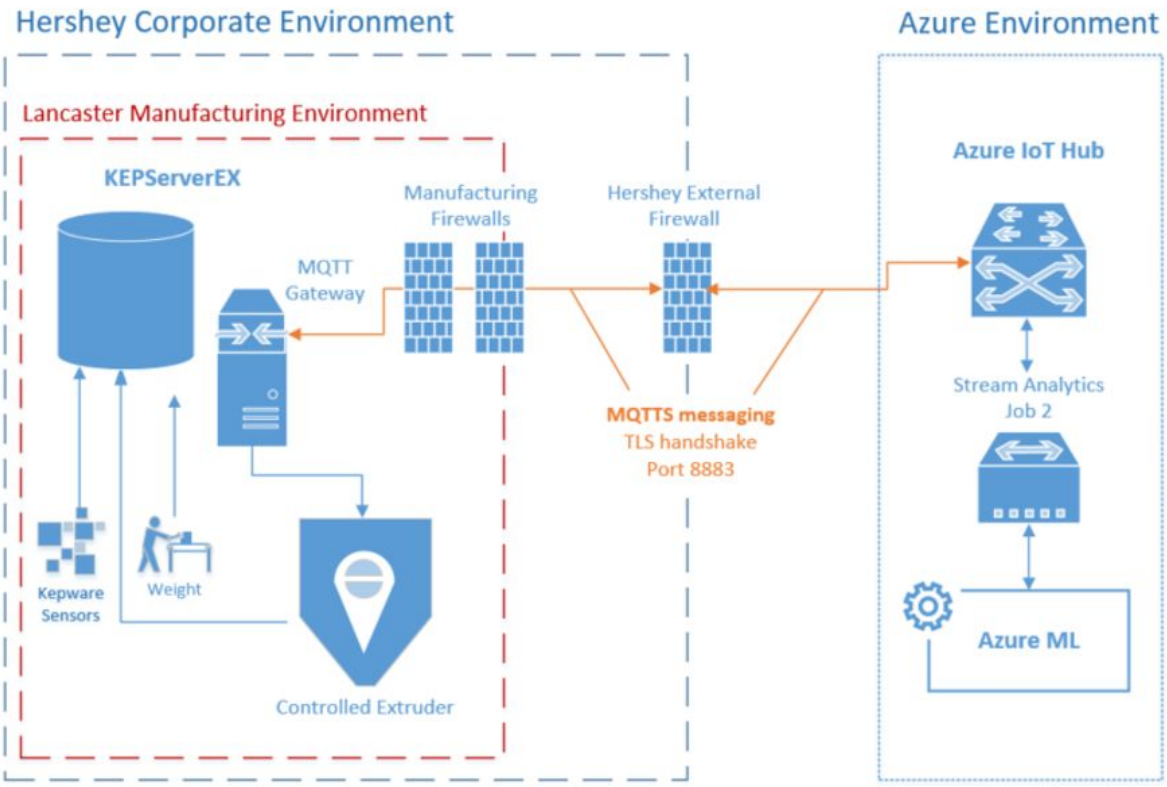
IoT Architecture: Typical Gateway Scenarios

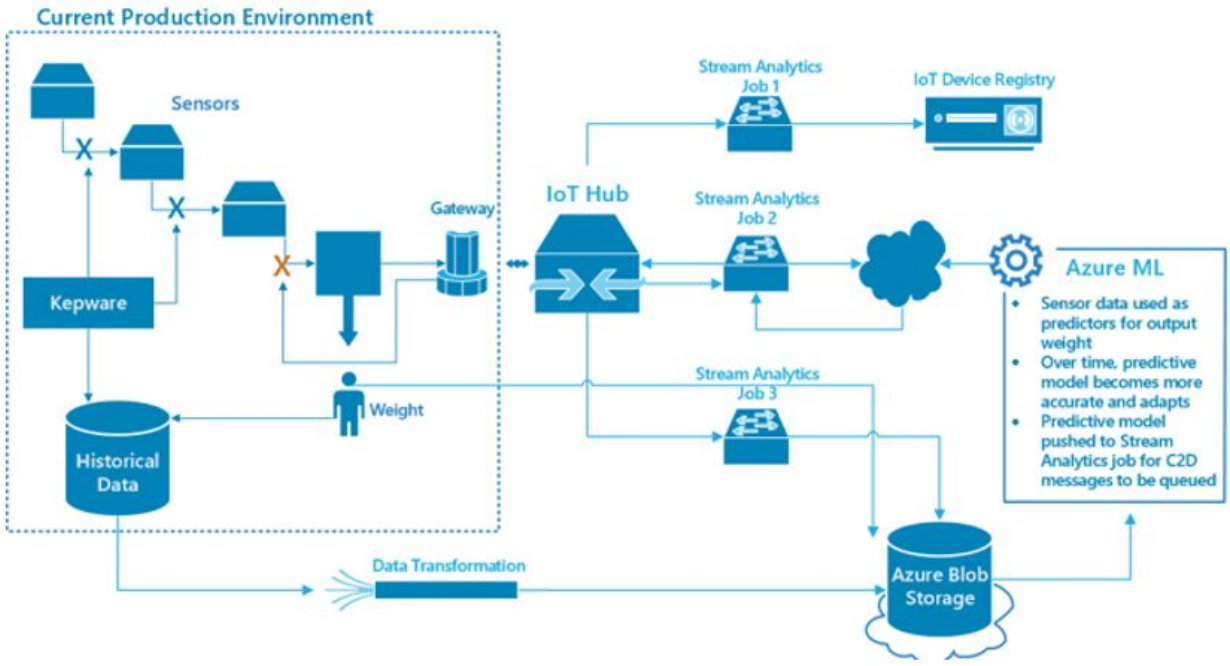


source: *Encapsulating Complexity in IoT Solutions*, Eurotech



Hershey IoT architecture design





*For reference: the Kepware server is the software controlling production line PLCs