Internet of Things

By John Patrick, ECE '18

Introduction

The Internet of Things is a newly emerging topic of technical, social, and economic significance. With its' applications stretching from basic consumer products to highly advanced sensors and industrial components, the Internet of Things promises to transform the way we live through the added benefits of network connectivity. Everyday objects such as lightbulbs, cars, and other goods can be transformed into powerful data analytics tools with this added network connectivity. Economic projections for the impact of IoT are anticipated as high as more than $11 trillion by 2025 [5].

As the Internet of Things (IoT) continues to grow and the number of IoT devices surges towards 100 billion by 2025, new risks and challenges are becoming more prevalent [5,6]. Connecting products such as cars, cameras, and industrial machines to the internet, raises new types of security concerns [6]. The act of hacking IoT devices, for example, is a topic that causes great concern for those relying on technological features of IoT devices to safely complete a task without risk of injury or even death [4]. At the same time, security concerns and privacy risks make everyday consumers of these IoT devices question whether their everyday lives may be monitored through the collected data analytics. As IoT technologies continue to evolve over time, we must wait and see whether these risks outweigh the potential gains provided by the network connected devices.

THING	+	IT (Hardware / Software)	=	Thing-based function (Physical / Local)	+	IT-based service (Digital / Global)
Bulb		IoT stack	→	Light		Security
Bin		IoT stack	→	Storage capacity		Automatic replenishment
Tractor		IoT stack	→	Towing vehicle		Predictive maintenance, optimization

Fig1 - IoT-product-services logic (based on Fleisch et al. 2014)

Current Applications

General Applications

Originally coined in 1999 by Kevin Ashton [4] to describe the connection of physical objects to the internet by sensors, the Internet of Things is not an entirely new idea. In 1999 the use of RFID tags to track and manage goods within factories without the need for human involvement proved to be groundbreaking [4]. With the realization of how useful and efficient these network connected devices could be, along with the decreasing costs, higher internet speeds, and the growth of large scale computing infrastructure, IoT technologies have spread to almost every field imaginable.

One common application that one may see on an everyday basis is the emergence of wearable technologies aimed at monitoring health and wellness; disease management, increased fitness, and greater productivity. In the home, office, and retail environments, buildings have begun to incorporate IoT enabled environment controllers, security systems, and even inventory optimization tools.

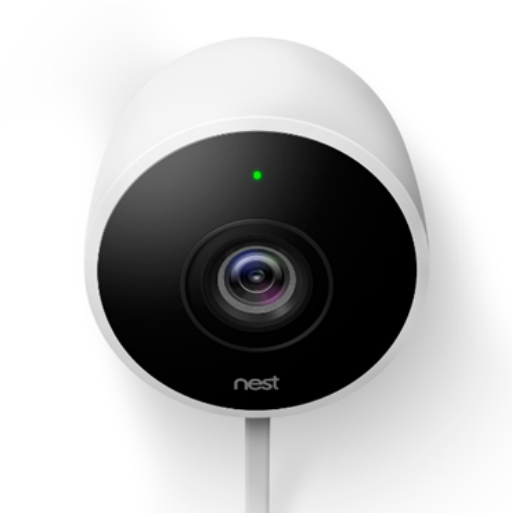

Fig2- nest security camera, capable of transmitting live video feed to wireless phone and alerting you when motion is detected. *Courtesy of NEST*

Medical Applications

The integration of the Internet of things into the medical world has been made possible largely in part due to advances in sensor and interconnect technologies. Deemed the internet of mobile health, the integration of medical sensors into mobile technology proves to be one of the most beneficial receptors of IoT technology [6,7]. More efficient methods of powering these medical devices continue to provide doctors with a way to monitor and diagnose their patients over an extended period without much oversight. With these advancements, wireless sensor-based systems can gather medical data that was never previously accessible. Dentists, for example, are beginning to take advantage of advanced bio-marker detection sensors to monitor and track what their patients are both putting into their mouths and how it is affecting their overall health. Dentists can determine whether the individual is at risk for cavities by tracking simple metrics such as the pH value of a patient's saliva. By utilizing the electrical properties of different biomaterials, such as graphene and carbon-nanotubes, researchers and scientists have started to develop smaller ion sensitive sensors to gather these metrics [2]. When paired with network connected devices, these sensors allow dentists to better understand how their patients are treating their teeth daily, and not just once every six months. In terms of our senior project, an electrode like thread pH sensor is connected wirelessly to a phone using a Bluetooth low energy connection. Therefore, instead of just directly measuring the output from the pH sensor, we can transmit and connect the sensor to a cellular device to more actively display and track our collected metrics.

In recent years, the application of Mobile Cloud Computing (MCC) in the medical field has helped to minimize the limitations of traditional medical treatment [7,8]. Since IoT devices rely on the collection of large amounts of data, internet connected medical devices previously lacking a way to store and process this information in a succinct and efficient manner faced issues such as overloading. Therefore, by moving the processing and storage capabilities to the cloud, mobile medical IoT devices have become much more capable. These more centralized and powerful computing capabilities not only help to limit the previously mentioned overloading issues, but also addresses problems with security and medical errors due to improperly processed data [8].

Future Problems

The attributes of many IoT implementations present new and unique security concerns. As this type of network connected technology becomes more integrated into our every day lives, it is imperative that the security, privacy, and safety of its users is taken into consideration. The interconnected nature of IoT devices means that every poorly secured device that is connected online not only affects the security of the user but also the internet as a whole. As IoT devices begin to form larger and larger interconnected networks, the risk for potential security damage is amplified [6].

IoT devices are at risk of being compromised by hackers like any online resource [6]. When one considers the idea that millions of people rely on IoT devices in products such as cars, security systems, and medical devices the risk for lifelong damage is

quickly amplified. Since many of the IoT devices being developed today rely on tracking the data collected by the users, the question of privacy becomes a huge priority [4].

When using IoT technologies, users want to be able to know that their identity and information being collected about them is safe from outside eyes. With the growth of large scale computing and data analytics, IoT users are becoming more cautious and wary about what they are willing to share. Not knowing what individual or company is seeing your information is enough, for many, to not purchase any form of IoT device.

References

1. F. Wortmann and K. Flüchter, "Internet of Things," *Business & Information Systems Engineering*, vol. 57, no. 3, pp. 221–224, Jun. 2015.

2. G. Tsuruzoe and K. Tsuchiya, "Development of the pH measurement sensor to be mounted on the oral measurement device," in *2016 International Symposium on Micro-NanoMechatronics and Human Science (MHS)*, 2016, pp. 1–1.

3. "The Role of Sensors in IoT Healthcare Applications | DigiKey." [Online]. Available: https://www.digikey.com/en/articles/techzone/2014/jul/the-role-of-sensors-in-iot-medical-and-healthcare-applications. [Accessed: 05-Dec-2017].

4. Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, June 2015.

5. "Global Connectivity Index." Huawei Technologies Co., Ltd., 2015. Web. 6 Sept. 2015. http://www.huawei.com/minisite/gci/en/index.html

6. Maple, C. (2017). Security and privacy in the internet of things. Journal of Cyber Policy, 2(2), 155–184. https://doi.org/10.1080/23738871.2017.1366536

7. Mora, H., Gil, D., Terol, R. M., Azorín, J., & Szymanski, J. (2017). An IoT-Based Computational Framework for Healthcare Monitoring in Mobile Environments. *Sensors*, *17*(10), 2302. https://doi.org/10.3390/s17102302

8. Dinh Hoang T., Lee Chonho, Niyato Dusit, & Wang Ping. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing*, *13*(18), 1587–1611. https://doi.org/10.1002/wcm.1203