Introducing the Internet of Things Department

Phillip A. Laplante
Penn State

Ben Amaba
IBM

Editors:
Phillip A. Laplante, Penn State; plaplante@psu.edu

Ben Amaba, IBM; baamaba@us.ibm.com

Welcome to the Internet of Things, a new department with the mission of presenting fresh ideas and applications from a practitioner point of view.

We're interested in showcasing articles about real, implemented Internet of Things (IoT) systems—not theoretical treatments or laboratory-based proofs of concept. There are all too many of the latter and not enough of the former.

This is especially true with academic papers about potential applications that seem very distant from the realities of implementation.

The articles we're interested in featuring can take many different forms, but here are some examples:

- Descriptions of deployed IoT systems, particularly in "surprising" application domains.
- Reports from workshops, panel discussions, and practice-focused roundtables of professionals and researchers.
- Surveys and reviews of tools for building IoT systems, including examples of deployed systems built using the tools.
- Thoughtful discussions of societal, legal, and ethical issues surrounding the deployment of IoT applications.

When building real systems, failure is inevitable. But we often learn more from these failures than from our successes. Therefore, we invite articles that share unsuccessful experiences or lessons learned from failed (or moderately successful) IoT system deployment. We realize that it might be difficult to expose failures to the public domain, but there are positive ways to do so.

IOT FOR HEALTHCARE PANEL DISCUSSION

The following is an example of one type of article we'd like to showcase. It's a report based on a two-hour panel discussion on IoT in healthcare, held at the NIST offices in Gaithersburg, Maryland on 30 August 2017. The panel was part of a one-day workshop on IoT sensors hosted by NIST and the IEEE Sensors Council. Column editor Phil Laplante was the moderator, and participants included column editor Ben Amaba and other experts with experience building and/or sponsoring deployed IoT healthcare applications. The other panelists were:

- Seth Carmody, cybersecurity program manager for the Center for Devices and Radiological Health (CRDH), serving as co-chair of CDRH's Cybersecurity Working Group;
- Venky Karuppanan, CEO of Teezle, a leading IoT platform company;
- Mansur Hasib, cybersecurity leader, keynote speaker, author, and media commentator;

Published by the IEEE Computer Society
1520-9202/18/$33.00 ©2018 IEEE

- Marc Wine, subject matter expert in many areas including federal health policy and technology innovation, health IT and informatics, mobile health applications, and the Nationwide Health Information Network; and
- Ken Blount, infrastructure project lead at Program Executive Office Healthcare Management Systems, Department of Defense.

The intention of this panel discussion was to harvest mindshare from these practitioners to provide guidance for those building IoT healthcare applications. The discussion consisted of opening statements, a set of prepared questions, and closing statements. For brevity, here we provide a few of the questions and highlights from the answers.

Where Is IoT for Healthcare on the Gartner Hype Cycle?

Panelists observed that the stages of Gartner's Hype Cycle for Emerging Technologies (see Figure 1) represent the changing status of a new technology from its introduction (technology trigger) through various aspects of overstated expectations and disillusionment with the slow pace of realizing the expectations, to the realization of the technology's true capabilities and realities (enlightenment), to productive creation and deployment of systems using the technology.

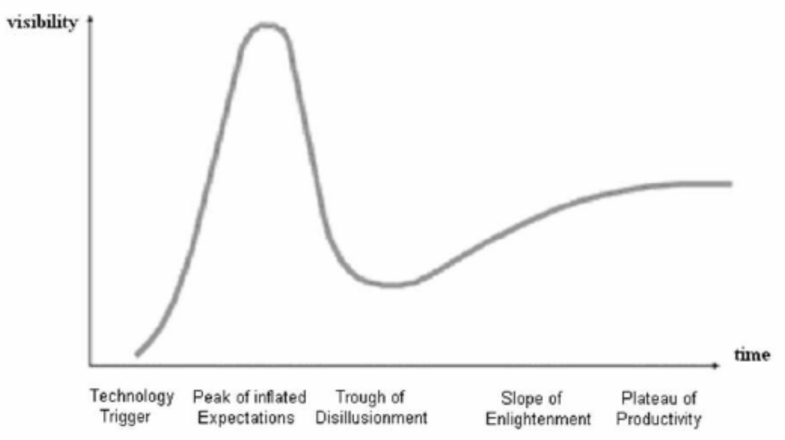

Figure 1. Simplified Gartner Hype Cycle.[1]

Panelists suggested that while IoT for healthcare is still somewhere between disillusionment and enlightenment, we need common standards, security (especially regarding human–machine interaction), interoperability, silo breakdowns, and a clearer definition of horizontal and vertical application layers to reach the plateau of productivity. Furthermore, we need a good data governance program, better requirements and architectures, and an improved understanding of human behavior.

IoT applications generate a lot of data, and the healthcare domain has a history of very advanced data collection, as opposed to other application domains that are beginning to enjoy the benefits of IoT. Panelists discussed the best uses of new kinds of data being collected by IoT applications. For example, there is clearly value in predictive, proactive analytics, so many companies will exploit this reality. But is there a business case for real-time reactive analytics that companies will pursue?

What Successes Have Been Achieved and What Lessons Have Been Learned?

Panelists noted that there have been many successes for IoT in the healthcare space. For example, patients can have certain organs such as the heart connected to the Internet through various types of monitors. The US National Kidney Registry uses IoT-enabled transport containers to track donor organ movement from harvest to implantation. Home telemedicine for veterans is being widely used by the US Department of Veterans Affairs and has potential for significant growth.

But several panelists wondered if we've done enough to create "trustworthy" healthcare systems. For example, it was recently shown that IoT-enabled devices that contain accelerometers for motion and location sensing can be disrupted through acoustic attacks.

What Challenges are Ahead?

Panelists agreed that there are many challenges, but that there's also a great deal to be learned from these challenges. For example, all panelists agreed that security, particularly for personal identifying information, is a big problem. One panelist noted that if an application employs "user id" and "password" on IoT healthcare applications, the consequences of loss or theft of this information could be deadly. To prevent unintended consequences, when an IoT medical device moves out of its intended context, alarms should be set off. A lesson learned from these observations is that we need continuous diagnostics in mitigation of cybersecurity.

Blockchain is widely thought to be a potential technology to provide security, privacy, and reliability in the IoT space. But panelists wondered if blockchain is ready for prime time.

Others noted that a huge challenge for IoT-enabled healthcare applications is opposition from organizations reluctant to expose their products and devices to the Internet because of security and intellectual property concerns. None of the medical IoT devices "speak the same language," which also arises partly from defending proprietary boundaries.

Medical devices need to be tamper-proof out of the box, but medical device experts shouldn't have to become cybersecurity experts. Similarly, every medical device and IoT healthcare solutions provider shouldn't need to be full-blown software companies. All of this means that we need off-the-shelf software components and solutions. One of the panelists suggested that licensing of software engineers working on critical infrastructure systems, as is done in many US states, would be essential for IoT-connected medical devices to ensure patient safety and privacy.

What Is Needed from Government/Industry/Academia to Move the Ball Forward?

Panelists pointed out that, in general, what is needed from all players comprises three categories: operational efficiency, better services, and applications that are closer to the customer. To achieve these goals, better information and experience sharing is essential. All 50 US states are supposed to share such information, but this isn't happening. Moreover, we need to share models (such as semantics models for data collection) and not just anecdotes, and we need to use this information in a meaningful way.

Platform standardization is another important area where progress needs to be made. It's unclear which platform vendor will emerge as the leader, but that leader will need to help companies build applications and monetize them, thus enhancing the virility of the platform.

Finally, we need to eliminate fragmentation among solutions and providers. Achieving this goal requires open data and open architecture standards. An iterative, actively engaged solutions development community is also needed.

CONCLUSION

Many of the panel's recommendations—the need for information sharing, open components and solutions, standardization, and learning from failures—reinforce the mission of our new department. We'd love to consider your contributions along these lines, but please query us before sending an article. Articles should be around 2,500 words (including figures and tables, which are considered 250 words each). Articles are reviewed by us and we might ask other experts to review it as well—submission is not a guarantee of publication. Because we have very limited editorial capability, submitted columns must be ready to go; that is, they must be well written and grammatically correct, and they must conform to the Computer Society's style guide (including all references in the correct format); see www.computer.org/cms/Computer.org/Publications/docs/2016CSStyleGuide.pdf. We look forward to reading your submissions!

REFERENCE

1. H.M. Jarvenpaa and S.J. Makinen, "An Empirical Study of the Existence of the Hype Cycle: A Case of DVD Technology," *IEEE Int'l Eng. Management Conference* (IEMC), 2008; doi.org/10.1109/IEMCE.2008.4617999.

ABOUT THE AUTHORS

Phillip A. Laplante is a professor of computer science at Penn State. Contact him at plaplante@psu.edu.

Ben Amaba is a Global Executive for the IBM Hybrid Cloud Division. Contact him at baamaba@us.ibm.com.