EDFAAO (2016) 3:18-21 1537-0755/$19.00 ©ASM International®

MANAGEABILITY CHALLENGES FOR INTERNET OF THINGS

Yen-Kuang Chen, Principal Engineer, Intel Corporation, and Associate Director, Intel-NTU Connected Context Computing Center
y.k.chen@ieee.org

There is no longer much argument around the Internet of Things (IoT) concept as the "next big thing," but consensus remains elusive around the next level of questions and discussion: Why is the IoT going to be so great, and what are the obstacles to achieving that vision?

The IoT is already delivering valuable benefits in the nascent stage of its development. However, I would argue that "IoT Version 1.0" has not yet been realized, and the magnitude of this revolutionary innovation will not become clear until then.

Getting to that point will require addressing a variety of user pain points, perhaps the most glaring of which is device failure. Mainstream adoption of and reliance on the IoT demands a scenario in which one or more disparate devices may fail but the overall system continues to function. Perhaps the system would not function as well as when the failed devices were operational, but it would continue. In the meantime, the failed device could be recognized and repaired without the user experiencing a disruption in service and with a return to optimal system performance.

In addition to more functionally reliable devices, IoT 1.0 will require an intelligent middleware layer for multivendor device management. Achieving such a layer will require global collaboration across the IoT's diverse stakeholders.

WHEN WILL THE IoT REALLY BE THE IoT?

I began working on the IoT six years ago, and at that time, I didn't have a clear definition of what the IoT is or would be.

Even today, different people have different definitions of the IoT. For some, the IoT is having things connected to a smartphone and enabling capabilities such as remotely locking/unlocking the front door. For others, the IoT is having a device connected to the internet, streaming data to the cloud, and having the cloud perform intelligent analytics to help humans make intelligent decisions. However, such definitions are still predicated on the notion of a small number of devices connected through the internet to individual humans, who, at the very least, are kept in the loop for all the real decision-making.

My definition of the true IoT—IoT 1.0, if you will—is when heterogeneous, multiple connected devices are working together to our benefit and without us having to make all of the decisions (Fig. 1). The IoT will deliver more benefits with more and more devices working together without human interaction, which both naturally impedes IoT scalability and adds complexity to our lives.

For example, mental wellness is an area that especially interests me. In the IoT 1.0, devices that measure various bio signals, such as heart rate and temperature, could be

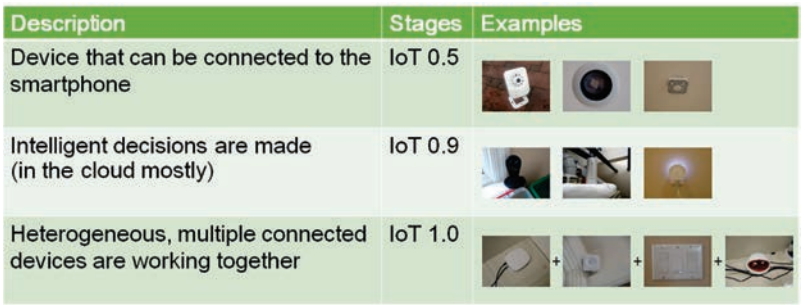


Fig. 1 When heterogeneous, multiple connected devices are working together without humans making all of the decisions, we will attain IoT 1.0.

in used in combination with other intelligence to better understand a person's mental as well as physical health state in relation to various stress factors. If a wearable sensor was linked with the user's calendar, the system may be able to connect the dots and realize that the reason a user is stressed is because there is a key meeting coming up in 15 minutes. Without the link to the calendar, while the device may be able to do numerous measurements of the human body, the overall system would not have any context for the results.

Another compelling use for the IoT 1.0 vision is the capability for devices to work together through the system to make someone (like me) more comfortable on a day when they are ill. Perhaps a device would note that my skin temperature is rising, detecting a fever, and know that I prefer a warmer room when I am feverish. With the IoT 1.0 providing a link between the device monitoring my temperature and the devices regulating climate control in my home, the system could adjust my environment to make it more comfortable without any direct interaction from me.

With the notion of multivendor, heterogeneous devices linked to one another and able to act in concert, the benefits of the IoT 1.0 for humans become quite easy to imagine. For example, we all have numerous keys, and many of us have garage-door openers, but do we really need these things in the emerging IoT world? Could a system recognize us and let us into our homes securely and conveniently without a key or garage-door opener? It would be great if, when my car approached the driveway of my home, the system sensed my approach and automatically opened the garage door. When I leave the house, it should be able to close the door, lock it automatically, and turn on the home-security systems, because it knows I am gone.

Across security and access control, utility management (lighting, electric vehicles, energy efficiency, garden and home appliances), healthcare and assisted living, audio/visual services, entertainment, and so on, the benefits to such a vision of the IoT are clear. However, challenges must be addressed to achieve an IoT 1.0 in which heterogeneous, multiple connected devices work together to my benefit without me controlling everything.

> "MY DEFINITION OF THE TRUE IoT—IoT 1.0, IF YOU WILL—IS WHEN HETEROGENEOUS, MULTIPLE CONNECTED DEVICES ARE WORKING TOGETHER TO OUR BENEFIT AND WITHOUT US HAVING TO MAKE ALL OF THE DECISIONS."

The single most problematic set of pain points inhibiting realization of the IoT 1.0 vision today may be device failures. Communication and battery issues can undo whole systems and their potential benefits. Plus, there's usually a limited user interface for debugging. Without a better solution for managing and adapting to device failure, the IoT will continue to be more of a technological novelty or curiosity than a major underpinning of daily life around the globe.

MY IoT@HOME

I recently counted over 100 commercially available connected devices in my house. *One hundred!* Presence sensors, motion sensors, electronic lock, lighting control, water sensors, garage-door opener, cameras, sirens, smart meters, smoke detectors, and so on (Fig. 2). For example, I have a very heavily connected and guarded front porch: four cameras, three motion sensors, three infrared lights,

Fig. 2 **In my IoT@Home, apps and devices provide benefits, but such a large number of devices creates the issue of device failure, which requires a significant amount of debugging time.**

and three open/close sensors. In addition, I use more than 20 apps in my home.

So many devices and so many apps unquestionably bring me a great deal of personal benefit; however, so many devices and apps create issues, too. The biggest challenge I face in my personal "IoT@Home" is that I constantly need to fix one thing or another. Each device has an approximate average failure rate of once per year. So, if just one device fails per week, that leaves me in a regular mode of debugging my system, and that keeps me really, really unhappy.

Device failures currently comprise a problem with only 100 devices in my home, but what happens when the forecasts for IoT proliferation come to pass and I have 300 or 400 connected devices in my home? Most home users simply are not interested or are incapable of dealing with each individual fault across devices in a system that is so quickly growing in complexity, interconnectivity, and the sheer number of devices.

TOWARD A SOFTWARE-DEFINED IoT

Implicit in the issue of device failures are at least a couple of calls to action for the industry that is building out the IoT 1.0 around the world. Device manufacturers can strive to make more-reliable devices, and, of course, they already are and always will be striving to do so. Certainly, this is a necessary pursuit.

However, even if devices are made more reliable, the truth is that some rate of device failure is inevitable. The IoT 1.0 will deliver its greatest benefits when users are able to experience the IoT while remaining almost naïve to the applications and devices that enable the experience. The system should still be able to operate, even when individual devices run into a faulty state.

This need tees up the requirement for an intelligent middleware to minimize human effort and automatically monitor and control the overall system, recognize individual failures, and hand over capabilities among devices as necessary. There needs to be an intelligent mapping of devices within the virtual space of the IoT 1.0. This cyber-physical intersection will be critical to a resilient system.

At the Intel-NTU Connected Context Computing Center, for example, we are working on a proactive management framework, "WuKong," that works to limit IoT user interaction to simply sending requests to applications and defining context and high-level policy. The new middleware layer intelligently maps the logical relationship to physical devices, and, when devices fail or are replaced, the middleware automatically re-maps a logical relationship to the physical devices (Fig. 3).

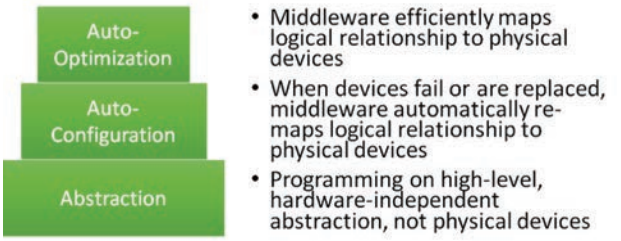


Fig. 3 Middleware will enable a software-defined IoT, minimizing human intervention.

Furthermore, programming is performed on high-level, hardware-independent construction—not the specific physical devices—so that programs can be written once and then run everywhere across the IoT. Moving the devices/services around becomes easier. Finally, if the user's intention is properly communicated to the middleware, then the user should not be concerned with finely adjusting the device sensitivities.

Sensitivity is another area of pain. For example, today a motion sensor set too sensitive on my front porch may detect a car passing on the street in front of my home and trigger useless picture-taking by my home-security system; the same motion sensor set not sensitive enough may ignore someone walking on my front yard. With a better, more intelligent middleware that understands the security goals of the user, the middleware should make sensitivity decisions per device based on the user's greater system-level intention, as opposed to simple, preset thresholds for each device.

Such a middleware layer is being designed ultimately to enable a software-defined IoT that would minimize human intervention and relieve the pain point of managing devices. It is one of the places where the IoT demands open, cross-discipline collaboration to rapidly and fully bring about the benefits envisioned. I invite you to visit http://iot.ieee.org/iot-scenarios.html to weigh in on the Intel-NTU Connected Context Computing Center's concept for intelligent IoT middleware and other emerging IoT scenarios.

CONCLUSION

Collaboration is the key for a large system such as the IoT 1.0 to function optimally. Many different components across diverse application domains must be able to seamlessly interoperate, and each application domain has insights that must be taken into account for the greatest potential benefit of the IoT to be realized. Technologies must and will advance so that the system is still able to operate even in the reality of device failure.

CALL TO ACTION

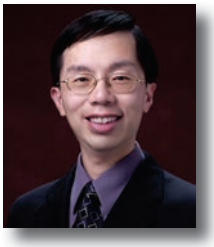
IEEE is a proven forum for stakeholders globally to collaborate for the benefit of humanity. IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity, with more than 426,000 members in more than 160 countries (over 50% of whom are from outside the United States).

The IEEE IoT Initiative (http://iot.ieee.org), for example, has released a document intended to establish a baseline definition of IoT in the context of applications that range from small, localized systems constrained to a specific location, to a large global system that is geographically distributed and composed of complex subsystems. The IEEE IoT Initiative invites global involvement from parties interested in advancing the definitions within the IoT.

In addition, the IEEE Standards Association has a number of standards, projects, and events that are directly related to creating the environment needed for a vibrant IoT (http://standards.ieee.org/innovate/iot/index.html).

Collaboration through such globally open activities will help ensure that the IoT indeed turns out to be the "next big thing."

ABOUT THE AUTHOR



Yen-Kuang Chen is a principal engineer at Intel Corporation. His research areas span from emerging applications that can utilize the true potential of the IoT to computer architecture that can embrace emerging applications. Dr. Chen has 60+ U.S. patents, 20+ pending patent applications, and 90+ technical publications. He is one of the key contributors to Supplemental Streaming SIMD Extension 3 and Advanced Vector Extension in Intel microprocessors. Dr. Chen has served as a program committee member of more than 50 international conferences on IoT, multimedia, video communication, image processing, VLSI circuits and systems, parallel processing, and software optimization. He is a steering committee member of *IEEE Internet of Things Journal*, the past chair of the IoT Special Interest Group of the IEEE Signal Processing Society, the Editor-in-Chief of *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, and the Distinguished Lecturer of the IEEE Circuits and Systems Society. Dr. Chen received his Ph.D. from Princeton University and is an IEEE Fellow.