Internet of Things
Making the Hype a Reality

Arpan Pal, *Innovation Lab, Tata Consultancy Services*

The Internet democratized information. The Internet of Things (IoT) will democratize knowledge. As industrial researchers who work with businesses, we at Tata Consultancy Services see our customers in every industry looking for ways to create active knowledge and insight from IoT data. Organizations wish to innovatively apply this data to new business models in which understanding and addressing customer needs and demands is the focus (not just the product or service, as it is now), culminating in an improved B2C or B2B2C value chain for most businesses. Is IoT technology geared up to meet the challenge? What can we do to make the IoT hype and prospects a reality? Toward this end, I identify six key interest areas we should pay attention to—*s*calability, *p*rivacy, *a*ffordability, *c*ontext-awareness, *e*ase-of-development, and *s*ecurity, or *SPACES*. I elaborate on each of these here.

Scalability: Leverage Computing at the Edge

The IoT is all about putting sensors on physical objects and humans and connecting them to monitor, diagnose, or predict physical states and events. It's predicted that 40 to 50 billion IoT devices will be connected to the Internet by 2020 (www.cisco.com/web/about/ac50/ac207/crc_new/university/RFP/rfp13078.html). So, can the infrastructure handle the deluge of data that these devices will churn out? Probably not.

Network scalability is the traditional way to look at this problem. Scalability would be required in every layer of the network. At the physical layer, we would need cognitive radio[1] and TV white space reuse to handle the spectrum crunch.[2] In upper layers, there is IETF 6LoWPAN to connect devices to IP networks (http://datatracker.ietf.org/wg/6lowpan/documents/), IPv6 to handle scalability at the network layer (http://ipv6.com/articles/organizations/IETF-History-IPv6.htm), and the IETF's Constrained Application Protocol (www.ipso-alliance.org), MQTT (http://mqtt.org), and ZeroMQ (http://zeromq.org) at the application layer to provide lightweight data transport. Going forward, adaptive systems[3] on top of software-defined[4] and information-centric networks (https://irtf.org/icnrg) will also play an important role.

However, there is a more elegant way to handle the scalability issue—instead of passing sensor data through the Internet via edge devices such as routers and gateways, this data can be processed and analyzed at the edge itself, utilizing the compute power already available in edge devices. This new paradigm is known as *fog computing*.[5] Incorporating the fog infrastructure into the IoT is important to provide the compute scalability needed for the real-timeness and latency predictability demanded by the IoT applications. However, the heterogeneity of edge compute nodes and their unpredictable availability poses interesting research challenges,[6] and that's in addition to the usual scalability required for storage and management of huge amounts of data.

Privacy: Make It Measurable

All the hype around the IoT will come to nothing unless privacy issues associated with the collected sensor data are addressed to the satisfaction of all stakeholders. The Holy Grail of privacy is to have data that's both contextually useful and forever privacy-preserving. In the complex ecosystem of the IoT, this is never going to happen, because there is a need for data sharing across multiple entities. Can we have a platform that can automatically ensure conformance to privacy regulations (https://www.privacyrights.org/topics/11)? Additionally, we should also look into giving insight to data owners about the potential for privacy breaches of shared data vis-a-vis the utility they're getting from the IoT applications that use this data. Providing a "privacy metric"[7]

Published by the IEEE Computer Society

to data owners that quantifies a potential privacy breach is one way to address this. However, the creation of such a metric depends on the data type and its intended use, and is hence quite complex to model.

Affordability: Crowdsourced Sensing

The return on investment for major IoT deployments isn't sufficiently motivating at this stage for most businesses. This is a primary reason why IoT applications have rarely moved beyond pilot deployments. There are deployment and cost issues when it comes to installing multitudes of sensing hardware across physical spaces. To make it more cost-effective, enterprises are looking into crowdsourcing sensing data from mobile phones where appropriate. Mobile phones are already pervasive, and they come with rich sensors such as cameras, microphones, accelerometers, gyroscopes, magnetometers, GPS, and altimeters. Participatory and opportunistic sensing using mobile phones will play a key role in IoT deployment.[8] A plethora of applications are possible using mobile phone sensors, prominent among them being road condition monitoring, driving behavior analysis,[9] traffic monitoring,[10] wellness/health monitoring, and so on.[11] In the future, robots and unmanned aerial vehicles carrying sensors will also contribute to this pervasive, affordable sensing paradigm.

Context-Awareness: What It Means for IoT Analytics

The IoT's real value will be realized only when we can derive physical contexts from the sensor data gathered. For sensors deployed on physical objects, this means answering questions such as what happened, where, when, and why. For sensors deployed on humans, the context means answering questions such as who is doing what, in where, or who is feeling what and why.[12] Thus, context-awareness in the IoT ultimately boils down to using analytics to detect a physical event, cause, identity, location, activity, physiology, and psychology from sensed data.

Ease of Development: Address Complexity

In the diverse IoT world, we can no longer afford to build vertical applications from scratch—a platform-based development approach promoting software re-use via APIs and services is a must.[13] Going further, one of the fundamental game-changers for successful IoT adoption will be the democratization of knowledge derived from IoT data. To make this happen, we need a crowdsourced application development and consumption ecosystem. Developing analytical applications for the IoT is a complex process that needs diverse knowledge of domains, sensors, algorithms, programming, and deployment infrastructure. A viable way to address such complexity is through a model-driven development (MDD) framework.[14] MDD is an approach that aims to model knowledge across different stakeholders (such as sensor providers, algorithm providers, domain experts, and infrastructure providers) by allowing separation of concerns for each stakeholder. It can assist an IoT application developer in easily creating an application based on data and goal descriptions.[15] Domain-agnostic semantic data interoperation[16,17] will also play a big role in such a framework.

Security: Why It's Different for the IoT

The security of anything IoT-related is one of the most talked-about concerns surrounding IoT applications. What does security mean in the IoT context? Is it any different or more complex than traditional IT systems? Fundamentally speaking, the answer is no. Security in IoT systems still means reliable data encryption before transmission and efficient management of the encryption key exchange. Of course, there is a scalability problem in distributing large numbers of keys across large numbers of devices. The resource constraints of sensing devices also add to this complexity. However, the real issue of IoT security isn't its implementation, but rather its implication. Because the IoT links the physical world to the cyberworld, any security breach in the cyberworld will affect the physical world and vice versa, leading to potentially catastrophic impacts.[18] Hence, we must look at IoT security in a more holistic manner, focusing on the minimization of such impacts.

The hype around IoT technology seems justified, given that it could disrupt many businesses. However, there are quite a few challenges that need to be addressed before the IoT becomes a reality and adds value to the business value chain. Quite a few end-to-end service integration platforms are being built to address one or more of the SPACES challenges I've discussed here (www.tcs.com/about/research/Pages/TCS-Connected-Universe-Platform.aspx).[19] Such platforms will play an extremely important role in the future successful deployment of IoT solutions. IT

References

1. M.A. Shah et al., "Cognitive Radio Networks for Internet of Things: Applications, Challenges and Future," *Proc. 19th Int'l Conf. Automation and Computing* (ICAC), 2013, pp. 1–6.

2. J. Temperton, "TV White Space Will Connect the Internet of Things," *Wired*, 13 Feb. 2015; www.wired.co.uk/news/archive/2015-02/13/white-space-spectrum.
3. S. Bandyopadhyay et al., "Adapting Protocol Characteristics of CoAP Using Sensed Indication for Vehicular Analytics," *Proc. 11th ACM Conf. Embedded Networked Sensor Systems*, 2013, article no. 48.
4. S. Fogarty, "7 Essentials of Software-Defined Networking," *Information Week Network Computing*, 19 Nov. 2013; www.networkcomputing.com/networking/7-essentials-of-software-defined-networking/d/d-id/898899.
5. B. Flavio et al., "Fog Computing and Its Role in the Internet of Things," *Proc. MCC workshop on Mobile Cloud Computing*, 2012, pp. 13–16.
6. S. Dey et al., "Challenges of Using Edge Devices in IoT Computation Grids," *Proc. Int'l Conf. Parallel and Distributed Systems* (ICPADS), 2013, pp. 564–569.
7. A. Ukil et al., "IoT-Privacy: To Be Private or Not to Be Private," *Proc. IEEE Conf. Computer Comm. Workshops*, 2014, pp. 123–124.
8. W.Z. Khan et al., "Mobile Phone Sensing Systems: A Survey," *IEEE Comm. Surveys & Tutorials*, vol. 15, no. 1, 2013, pp. 402–427.
9. A. Ghose et al., "Road Condition Monitoring and Alert Application: Using In-Vehicle Smartphone as Internet-Connected Sensor," *Proc. IEEE Int'l Conf. Pervasive Computing and Comm. Workshops*, 2012, pp. 489–491.
10. T. Chakravarty et al., "MobiDriveScore—A System for Mobile Sensor-Based Driving Analysis: A Risk Assessment Model for Improving One's Driving," *Proc. 7th Int'l Conf. Sensing Technology* (ICST), 2013, pp. 338–344.
11. A. Pal et al., "A Robust Heart Rate Detection Using Smartphone Video," *Proc. 3rd ACM MobiHoc Workshop on Pervasive Wireless Healthcare*, 2013, pp. 43–48.
12. P. Charith et al., "Context Aware Computing for the Internet of Things: A Survey," *IEEE Comm. Surveys & Tutorials*, vol. 16, no. 1, 2013, pp. 414–454.
13. P. Balamuralidhara et al., "Software Platforms for Internet of Things and M2M," *J. Indian Inst. of Science*, vol. 93, no. 3, 2013, pp. 487–498.
14. P. Patel et al., "A Model-Driven Development Framework for Developing Sense-Compute-Control Applications," *Proc. 1st Int'l Workshop Modern Software Eng. Methods for Industrial Automation*, 2014, pp. 52–61.
15. A. Pal et al., "Model-Driven Development for Internet of Things: Towards Easing the Concerns of Application Developers," *Proc. Int'l Conf. IoT as a Service*, 2014.
16. *Semantic Sensor Network XG Final Report*, tech. report 28, W3C Incubator Group, June 2011.
17. D. Pfisterer et al., "SPITFIRE: Towards a Semantic Web of Things," *IEEE Comm. Magazine*, Nov. 2011, pp. 40–48.
18. E. Naone, "Hacking the Smart Grid," *Technology Rev.*, 2 Aug. 2010; www.technologyreview.com/news/420061/hacking-the-smart-grid/.
19. J. Gubbi et al., "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Elsevier J. Future Generation Computer Systems*, vol. 29, 2013, pp. 1645–1660.

Arpan Pal *is a principal scientist with Tata Consultancy Services, where he heads cyber-physical-systems research at the Innovation Lab, Kolkata. His current research interests include mobile phone and camera-based sensing and analytics, physiological sensing, M2M communications, and Internet-of-Things-based platforms and systems. Pal has more than 65 publications in reputed journals and conferences, has filed for more than 60 patents, and has nine patents granted to him. Contact him at arpan.pal@tcs.com.*