ISSN:2379-3686 International Journal Of Science Research And Technology Volume 2 Issue 3,PP 35-41, 25th December 2016

INTERNET OF THINGS; A HELICOPTER VIEW

Dr. Bhargavi Goswami,
Head, Associate Professor, Garden City College
Bangalore, India.

Abstract—Ubiquitous sensing enabled by Wireless Sensor Network (WSN) technologies cuts across many areas of modern day living. This offers the ability to measure, infer and understand environmental indicators, from delicate ecologies and natural resources to urban environments. The proliferation of these devices in a communicating–actuating network creates the Internet of Things (IoT), wherein sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms in order to develop a common operating picture (COP). IoT has stepped out of its infancy and is the next revolutionary technology in transforming the Internet into a fully integrated Future Internet. This paper presents a variety of tools and techniques used for implementing IoT giving clear idea to the readers of this paper showing roadmap to the fundamental of Internet of Things.

Keywords—component; formatting; style; styling; insert (key words)

I. Introduction (Heading 1)

This paper addresses the Internet of Things. Main enabling factor of this promising paradigm is the integration of several technologies and communications solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are just the most relevant. As one can easily imagine, any serious contribution to the advance of the Internet of Things must necessarily be the result of synergetic activities conducted in different fields of knowledge, such as telecommunications, informatics, electronics and social science. In such a complex scenario, this survey is directed to those who want to approach this complex discipline and contribute to its development. Different visions of this Internet of Things paradigm are reported and enabling technologies reviewed. What emerges is that still major issues shall be faced by the research community. The most relevant among them are addressed in details.

With the development of sensor, wireless mobile communication, embedded system and cloud computing, the technologies of Internet of Things have been widely used in logistics, Smart Meter, public security, intelligent building and so on. Because of its huge market prospects, Internet of Things has been paid close attention by several governments all over the world, which is regarded as the third wave of information technology after Internet and mobile communication network. Bridging between wireless sensor networks with traditional communication networks or Internet, IOT Gateway plays an important role in IOT applications, which facilitates the seamless integration of wireless sensor networks and mobile communication networks or Internet, and the management and control with wireless sensor networks. In this paper, we also describe IOT Gateway

system based on Zigbee and GPRS protocols according to the typical IOT application scenarios and requirements from telecom operators, presented the data transmission between wireless sensor networks and mobile communication networks, protocol conversion of different sensor network protocols, and control functionalities for sensor networks, and finally gave an implementation of prototyping system and system validation.

II. Few Examples

Although the concept wasn't named until 1999, the Internet of Things has been in development for decades. The first Internet appliance, for example, was a Coke machine at Carnegie Melon University in the early 1980s. The programmers could connect to the machine over the Internet, check the status of the machine and determine whether or not there would be a cold drink awaiting them, should they decide to make the trip down to the machine.

At the University of Washington, the RFID ecosystem creates a microcosm for the Internet of Things. The authors developed a suite of Web-based, user-level tools and applications designed to empower users by facilitating their understanding, management, and control of personal RFID data and privacy settings. They deployed these applications in the RFID ecosystem and conducted a four-week user study to measure trends in adoption and utilization of the tools and applications as well as users' qualitative reactions.

A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), microservices and the Internet. The convergence has helped tear down the silo walls between operational technology (OT) and information technology (IT), allowing unstructured machine-generated data to be analyzed for insights that will drive improvements[1].

Kevin Ashton, cofounder and executive director of the Auto-ID Center at MIT, first mentioned the Internet of Things in a presentation he made to Procter & Gamble in 1999. Here's how Ashton explains the potential of the Internet of Things: "Today computers -- and, therefore, the Internet -- are almost wholly dependent on human beings for information[2]. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code[3].

The problem is, people have limited time, attention and accuracy -- all of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things -- using data they gathered without any help from us -- we would be able to track and count everything and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling and whether they were fresh or past their best."

IPv6's huge increase in address space is an important factor in the development of the Internet of Things. According to Steve Leibson, who identifies himself as "occasional docent at the Computer History Museum," the address space expansion means that we could "assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do

another 100+ earths." In other words, humans could easily assign an IP address to every "thing" on the planet[4]. An increase in the number of smart nodes, as well as the amount of upstream data the nodes generate, is expected to raise new concerns about data privacy, data sovereignty and security.

III. resets software, business models using IoT

The "Internet of Things" is becoming a reality, but a worldwide network of embedded sensors won't reach its potential without monetized software ecosystems and wireless networks that can easily cross national borders, according to panelists at this week's SAP Sapphire conference in Orlando, Fla.

In a discussion titled "The Internet of Things is Now," SAP sought to showcase customers who are implementing the technology[5,6]. Often referenced in the same breath as machine to machine (M2M), it typically involves giving machines and sensors unique identifiers so they can communicate with each other to automate processes without human intervention, while producing petabytes of big data that can be harnessed by control systems or crunched by analytics software[7].

"It has been limited to very high-value assets and specific verticals like oil and gas," said panel moderator Suhas Uliyar, SAP's vice president and general manager of Internet of Things/M2M. "But we are reaching an inflection point right now." Uliyar said Moore's Law is driving down the cost of sensors and communications, while telecom companies are starting to focus on building the necessary wireless networks[8].

One such telecom manufacturer is Ericsson, based in Stockholm, Sweden. "Many of the pieces of the puzzle are coming into place," said Jonas Bengtsson, Ericsson's director for new business development and innovation. Several years ago, Ericsson predicted there would be 50 billion connected devices in the world, and rapid growth in the last 12-18 months has made that goal achievable, Bengtsson said. "M2M represents, to us, the start of what we call the third wave of connectivity," with the first wave connecting places, and the second wave, people.

Two panelists said they have started putting sensors on equipment but are struggling to figure out what kind of software and business processes are required for analyzing the data and, ultimately, generating revenue. "We've found the engineering not that complicated," said Paul Wellman, CIO of Tennant Co., a Minneapolis-based manufacturer of commercial cleaning equipment. "It's manageable."

Tennant has attached "black boxes" that gather data on temperature, usage, and other variables from approximately 300 pieces of equipment in the United States and Canada. "The infrastructure and the engineering of the M2M solutions is proven. It's now become an issue of business intelligence and analytics." Tennant's marketing department is leading the charge, he said, because the top priority is deciding how to turn equipment service into a strategic value and price it properly.

Mikkel Sorensen, business developer for Grundfos Connect, a division of the Danish pump manufacturer, Grundfos, said his company also realized it needed a software ecosystem to take advantage of the sensors it has installed. "It's about connecting all the dots," he said.

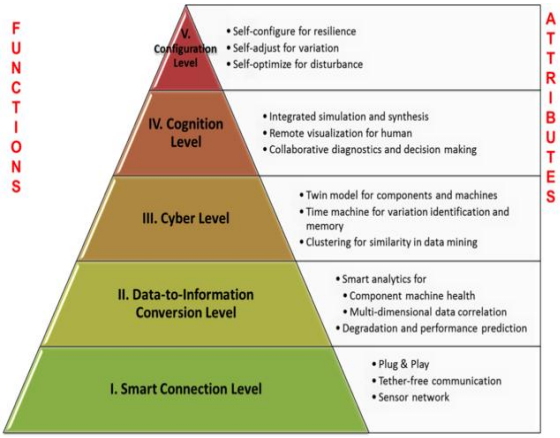
Sorensen said the system will allow Grundfos to offer servicing for competing brands, which also presents new sales opportunities. "It's a complete mindset change," he said.

Bengtsson called attention to another hurdle that is partly driven by software. "Telecom licenses are national at best," he said, and in the U.S., they can be

state by state. Ericsson is beginning to tackle such issues, he said. Uliyar later noted that standards bodies have begun to coordinate their efforts, which could help with cross-border interoperability[9].

Uliyar asked the panel if there were potential downsides to the Internet of Things. Sorensen warned that issues of security and privacy will arise in connection with data coming from devices. Hackers could see when water flowing into a home has been shut down for conservation reasons and deduce that no one is home. "If you're monitoring the water data at a Coca-Cola plant, you could actually predict their output," he said, and from that information, possibly surmise financial performance.

An audience member pointed out that having more control over pumps could give Grundfos a level of control that might make some customers uncomfortable. Sorensen responded that the same metering capability would allow the company to offer service level agreements (SLAs) like network service providers[9,10].



IV. Things aren't so simple

In an interview after the panel, Wellman said he has been asking SAP whether the sensor data can be integrated to SAP's enterprise asset management (EAM) module, where maintenance is often managed. "We use the service-order management in SAP ECC [ERP], he said.

Making equipment data accessible to an EAM system is a typical scenario, according to Henry Morris, senior vice president of worldwide software and services research at analyst firm IDC, based in Framingham, Mass. "The EAM system is going to be the hub of what you're going to do with these capital assets," Morris said. "That's what SAP has to do with this."

Morris, who was in the audience for the panel discussion, said IDC surveys indicate that companies are recognizing that sensors are a bigger opportunity in big data than personal data from credit cards and social media. IDC is also starting to see real applications of the technology, Morris said. "They're predicting not how people will behave, but how objects will perform."

V. What is IOT

What is the Internet of Things, exactly? It is an ambiguous term, but it is fast becoming a tangible technology that can be applied in data centers to collect information on just about anything that IT wants to control.

The Internet of Things (IoT) is essentially a system of machines or objects outfitted with data-collecting technologies so that those objects can communicate with one another. The machine-to-machine (M2M) [15] data that is generated has a wide range of uses, but is commonly seen as a way to determine the health and status of things -- inanimate or living.

IT administrators can use the IoT for anything in their physical environment that they want information about. In fact, they already do[11].

In one case, IoT is being used to stymie deforestation in the Amazon rainforest. A Brazilian location-services company called Cargo Tracck places M2M sensors from security company Gemalto in trees in protected areas[12]. When a tree is cut or moved, law enforcement receives a message with its GPS location,

allowing authorities to track down the illegally removed tree.

One analyst explained the IoT using the iPhone as an analogy. Disconnected third-party applications that are hosted in the cloud can be connected, and users can access all sorts of data from the device, according to Sam Lucero, senior principal analyst, M2M and Internet of Things, at IHS Electronics & Media in Tempe, Ariz[13].

VI. How IOT Works

While some consider IoT to be M2M communication over a closed network, that model is really just an intranet of things, Lucero said.

With an Intranet of Things, apps are deployed for a specific purpose and don't interact outside of that network. The true IoT is where different applications are deployed for specific reasons and the data collected from the machines and objects being monitored are made available to third-party applications. The expectation is that true IoT will provide more value than what can be derived from secluded islands of information, Lucero said[14].

For the IoT to work in data centers, platforms from competing vendors need to be able to communicate with one another. This requires standard APIs that all vendors and equipment can plug into, for both the systems interfaces as well as various devices, said Mike Sapien, a principal analyst with Ovum.

IBM proposed in February that its IoT protocol, called Message Queuing Telemetry Transport (MQTT), be used as the open standard. This would help multiple vendors participate in the IoT.

"[System integrators] like HP, IBM and others are starting to open up their systems to be less restrictive, just as telecom operators are allowing different networks—not just their own—to be part of the IoT ecosystem," Sapien said. "But this has taken many years to happen."

Meanwhile, a number of platforms serve as the plumbing to connect systems from different vendors so that they can communicate and be managed. One such platform is Xively Cloud Services, which is LogMeIn Inc.'s public IoT Platform as a Service. It allows IT to design, prototype and put into production any Internet-connected device.

For example, companies that have to monitor energy use might use closed, vendor-specific systems. They can use something like Xively as a secondary system to monitor heating and cooling and control energy use across multiple locations.

Over the long term, one consequence of the Internet of Things for the enterprise data center could be a large volume of incoming data coming that requires significant infrastructure upgrades, particularly for data processing and storage, Lucero said.

VII. IOT Risks

In this article, further we will discuss the proliferation of the Internet of Things and explore what enterprises can do to manage the security risks associated with IoT devices.

With the rise of technologies such as software-defined networking, hyper-converged infrastructure and the Internet of Things, customers are facing new security vulnerabilities as the attack surface of their IT environment shifts in dramatic ways[16].

To help channel partners address these issues, we conducted interviews with several key industry executives who discussed how these technologies are changing the security landscape, identified important security weaknesses and shared tips on how to strengthen a customer's security posture.

In this IT security tutorial, we examine Internet of Things (IoT), an environment in which objects -- a

vehicle with built-in sensors, for example -- have network connectivity and can communicate and exchange data with Internet-enabled devices and systems.

The number of endpoints: By networking objects such as cars, buildings, factory facilities, homes, refrigerators, among others, a corresponding expansion in the number of endpoints that are vulnerable to data intrusion occurs, requiring a security posture that monitors more objects, devices and data across the network.

According to Jerome Buvat, Capgemini Consulting's expert in digital transformation and strategy, vulnerabilities for IoT or connected devices can come from multiple sources, such as the end-point device itself, the communication channel or the remote updates being deployed on the end-point devices.

Object/system design: Most objects or systems that are now connected to the Internet were not designed to be secured in a connected environment, Buvat said. For instance, in the case of cars, the on-board systems were designed to be wired and were reasonably secure to that purpose or use. However, as cars are being increasingly connected through wireless plug-in devices -- which may not even require authentication -- devices become vulnerable to cyberthreats.

Lack of standards: There are few standards that govern how to securely connect objects that have network connectivity to a company's enterprise, said Mark Jacobsohn, senior vice president at Booz Allen Hamilton, who oversees the firm's investment in the Internet of Things[17].

Connections to mobile devices: Rob Chee, principal security architect at Force 3, a network security company based in Crofton, Md., said many objects connected to the network are monitored and managed using apps on mobile devices[18]. Having mobile devices connected to IoT creates a further expansion of the attack surface. Companies will have to examine how mobile devices plug into IoT and consider security around the apps they use to control objects and the data that's collected from IoT sensors.

VIII. CONCLUSION

In summary I would like to mention that we are in the early stages in the creation of an Internet of Things and the above examples provide just a glimpse into what is possible when you combine sensors, actuators, and networked intelligence.

The #IoT is expected to also make impacts in government, education, finance and transportation. On the consumer side there are nearly endless combinations of applications. As an example, is there a reason why when a fire alarm goes off in your home it just beeps, instead of talking to your gas appliances to shut them off and making sure you wake up with an alert sent to your household phones?

When data is removed from soloed warehouses and is able to be identified and shared between products and services like it is within the current Internet architecture a true Internet of Things can emerge.

This paper is an effort towards broadening the vision and understanding of Internet of Things (IOT) for the beginners that will surely motivate and develop their research interest in the direction of IoT. With this paper, the one who don’t know anything about IOT will surely get helicopter view of the technology.

IX. Acknowledgment

I would like to show my gratitude to the support and knowledge sharing of John Moore, Nicole Lewis, David Linthicum, Bridget Botelho and all other people I referred their name in the relevant innovation and contribution they made to IoT. I would also like to thank the online researchers who shared their view with me while writing this survey article.

REFERENCES

[1] Bridget Botelho. IoT analytics guide: Understanding Internet of Things data. IOT Agenda,TechTarget.http://internetofthingsagenda.techtarget.com/feature/Explained-What-is-the-Internet-of-Things

[2] David Linthicum. IoT analytics guide: From Evolution to Revolution. IOT Agenda,TechTarget. http://internetofthingsagenda.techtarget.com/podcast/From-evolution-to-revolution-with-the-Internet-of-Things

[3] Complete RFID Analysis and Forecasts, 2008, [online] Available: online

[4] T. Kriplean, "Physical Access Control for Captured RFID Data", IEEE Pervasive Computing, vol. 6, no. 4, pp. 48-55, 2007

[5] H Gohel, "Introduction to Network & Cyber Security",LAP Lambert Academic Publishing, 2015

[6] V. Rastogi, "Access Control over Uncertain Data", Proc. 34th Int'l Conf. Very Large Databases (VLDB 08), pp. 821-832 [CrossRef]

[7] E. Welbourne, "Cascadia: A System for Specifying, Detecting, and Managing RFID Events", Proc. 6th Ini'l Conf. Mobile Systems, Applications and Services (MobiSys 08), pp. 281-294 [CrossRef]

[8] J. Hightower, "Learning and Recognizing the Places We Go", Proc. 7th Int'l Conf. Ubiquitous Computing (Ubicomp 05), vol. 3660, pp. 159-176 [CrossRef]

[9] H Gohel, B Goswami,"Intelligent Tutorial Supported Case Based Reasoning E-Learning Systems",Souvenir National Conference on Emerging Trends in Information & Technology & Management (NET-ITM-2011), 2011

[10] A. Juels, "RFID Security and Privacy: A Research Survey", IEEE J. Selected Areas in Comm., vol. 24, pp. 381-394, 2006

[11] M. Langheinrich, Personal and Ubiquitous Computing, 2008, Springer

[12] A. Nemmaluri, "Sherlock: Automatically Locating Objects for Humans", Proc. 6th Ini'l Conf. Mobile Systems, Applications and Services (MobiSys 08), pp. 187-198 [CrossRef]

[13] M. Philipose, "Inferring Activities from Interactions with Objects", IEEE Pervasive Computing, vol. 3, no. 4, pp. 10-17, 2004

[14] E. Welbourne, "Longitudinal Study of a Building-Wide RFID Ecosystem", Proc. 7th Int'l Conf. Mobile Systems, Applications, and Services (Mobicomp)

[15] Gohel H, Bhatia S, "Applied ICT - Beyond oceans and Spaces", LAP Lambert Academic Publishing, 2017

[16] ITU, "ITU Internet Reports 2005: The Internet of Things", The Internet of Things, Nov. 2005.

[17] Q. Liu, L. Cui, HM. Chen, "Key technologies and applications of Internet of Things", Computer Science, Vol. 37, No. 6, 2010.

[18] ETSI M2M Standardization, http://www.etsi.org/Website/Technologies/M2M. aspx

[19] Gohel H, "Li-Fi Technology–A survey on Current IT Trends" International Journal on Advances in Engineering Technology and Science,2015.

[20] H. Jin, WC. Liu, JT. Han and YL Ding, "Application Study of Internet of Things in Home", Telecommunications Science, Vol. 26, No. 2, 2010.

[21] D. Guinard and V. Trifa, "Towards the Web of Things: Web Mashups for Embedded Devices", in 2nd Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 2009), Madrid, Spain, April 2009.

[22] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A Survey", Computer Networks, Vol. 54, No. 15, pp. 2787-2805, Oct. 2010.