INTERNET OF THINGS - MODELS AND APPLICATIONS

S. Sravani[1], P. Udayasri [2], G. Priyanka [3]
P.G. Student, Department of CSE, SVU College of Engineering, Tirupati, India[1]
P.G. Student, Department of CSE, SVU College of Engineering, Tirupati, India[2]
P.G. Student, Department of CSE, SVU College of Engineering, Tirupati, India[3]

Abstract
Today, smart grid, smart homes, smart water networks, intelligent transportation, are infrastructure systems that connect our world more than we ever thought possible. The common vision of such systems is usually associated with one single concept, the internet of things (IoT), where through the use of sensors, the entire physical infrastructure is closely coupled with information and communication technologies; where intelligent monitoring and management can be achieved via the usage of networked embedded devices.

Keywords: Device-Device, Device-cloud, Device-Gateway, Back-end Data-Sharing

Introduction

The Internet of Things (IoT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the specialty press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. An abundance of conferences, reports, and news articles discuss and debate the prospective impact of the "IoT revolution"—from new market opportunities and business models to concerns about security, privacy, and technical interoperability.The large-scale implementation of IoT devices promises to transform many aspects of the way we live. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the "smart home'', offering more security and energy efficiency. Other personal IoT devices like wearable fitness and health monitoring devices and network enabled medical devices are transforming the way healthcare services are delivered. This technology promises to be beneficial for people with disabilities and the elderly, enabling improved levels ofindependence and quality of life at a reasonable cost.1 IoT systems like networked vehicles, intelligent traffic systems, and sensors embedded in roads and bridges move us closer to the idea of "smart cities'', which help minimize congestion and energy consumption. IoT technology offers the possibility to transform agriculture, industry, and energy production and distribution by increasing the availability of information along the value chain of production using networked sensors. However, IoT raises many issues and challenges that need to be considered and addressed in order for potential benefits to be realized.A number of companies and research organizations have offered a wide range of projections about the potential impact of IoT on the Internet and the economy during the next five to ten years. Cisco, for example, projects more than 24 billion Internet–connected objects by 2019[2]; Morgan Stanley, however, projects 75billion networked devices by 2020[3]. Looking out further and raising the stakes higher, Huawei forecasts 100billion IoT connections by 2025[4]. McKinsey Global Institute suggests that the financial impact of IoT on the global economy may be as much as $3.9 to $11.1 trillion by 2025[5]. While the variability in predictions makes any specific number questionable, collectively they paint a picture of significant growth and influence.Fundamentally, the Internet Society cares about the IoT as it represents a growing aspect of how people and institutions are likely to interact

with the Internet in their personal, social, and economic lives. If even modest projections are correct, an explosion of IoT applications could present a fundamental shift in how users engage with and are impacted by the Internet, raising new issues and different dimensions of existing challenges across user/consumer concerns, technology, policy and law. IoT also will likely have varying consequences in different economies and regions, bringing a diverse set of opportunities and challenges across the globe.

Internet of Things: Communications Models

Here, we outline framework of four common communication models used by IoT devices. Thisframework explains key characteristics of each model in the framework.

1. Device-to-Device Communications

In device-to-device communication model, two or more devices directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. However these devices use protocols like Bluetooth, Z-Wave, or ZigBee to establish direct device-to-device communications.

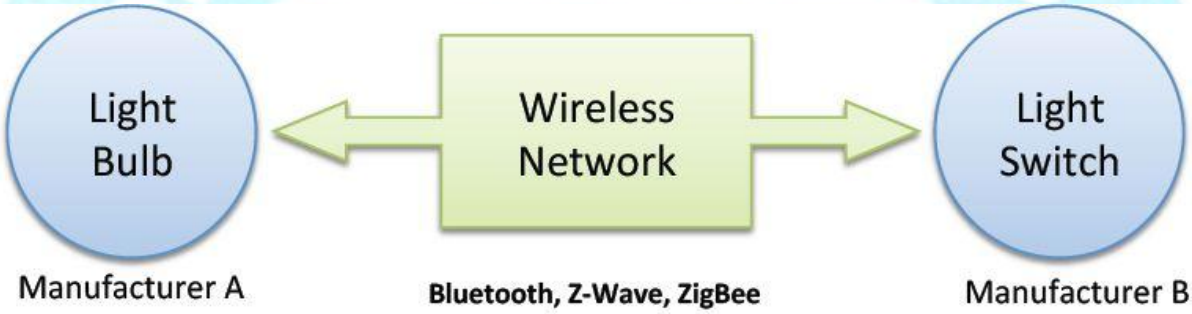

Fig 1:Example of device-to-device communication model.

These device-to-device networks allow devices that adhere to a particular communication protocol to communicate and exchange messages to achieve their function. This communication model is commonly used in applications like home automation systems, which typically use small data packets of information to communicate between devices with relatively low data rate requirements. Residential Iota devices like light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other(e.g. a door lock status message or turn on light command) in a home automation scenario.

2. Device-to-Cloud Communications

In a device-to-cloud communication model, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service.

Fig 2:Device-to-cloud communication model diagram.

However, interoperability challenges can arise when attempting to integrate devices made by different manufacturers. If proprietary data protocols are used between the device and the cloud service, the device owner or user may be tied to a specific cloud service, limiting or preventing the use of alternative service providers.

3. Device-to-Gateway Model

In the device-to-gateway model, or more typically, the device-to-application-layer gateway (ALG) model, theist device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation.

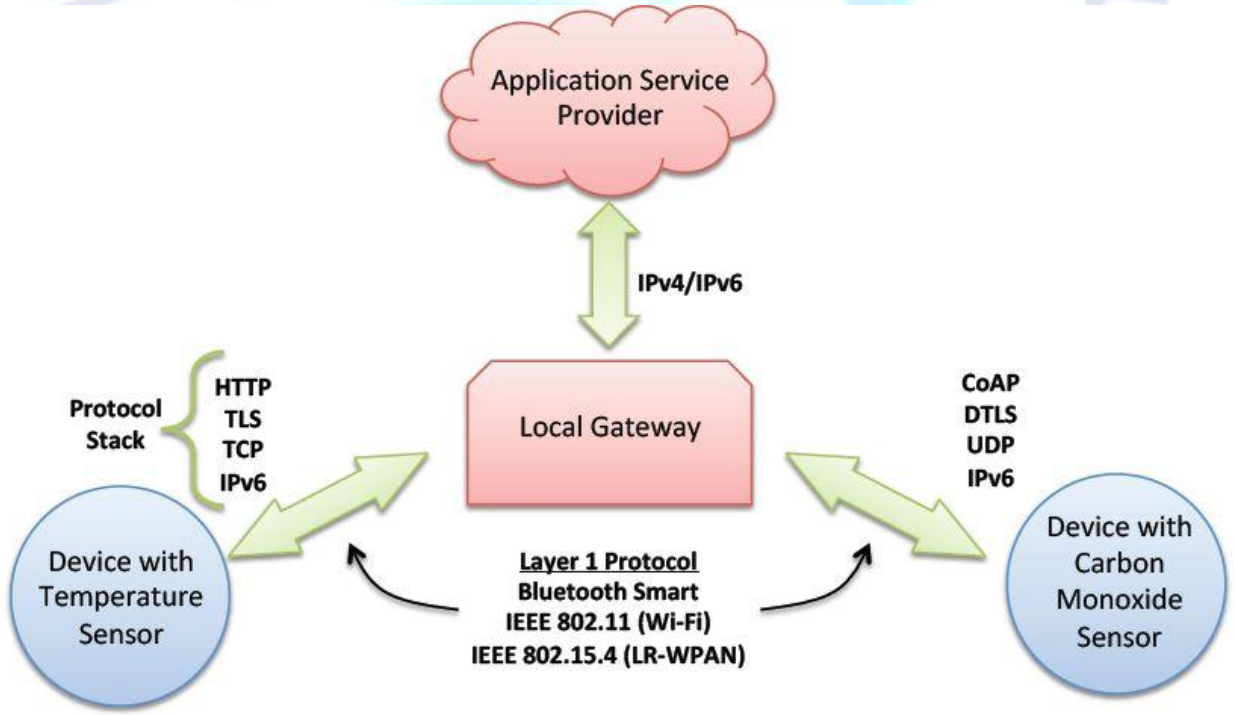

Fig 3: Device-to-gateway communication model diagram.

Several forms of this model are found in consumer devices. In many cases, the local gateway device is smartphone running an app to communicate with a device and relay data to a cloud service. This is often the model employed with popular consumer items like personal fitness trackers. These devices do not have the native ability to connect directly to a cloud service, so they frequently rely on smartphone app software to serve as an intermediary gateway to connect the fitness device to the cloud.

4. Back-End Data-Sharing Model

The back-end data-sharing model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. This architecture supports the desire for granting access to the uploaded sensor data to third parties. This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where Io T devices upload data only to a single application service provider. A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed. The back-end data-sharing model suggests a federated cloud services approach or cloud applications programmer interfaces (APIs) are needed to achieve interoperability of smart device data hosted in the cloud.

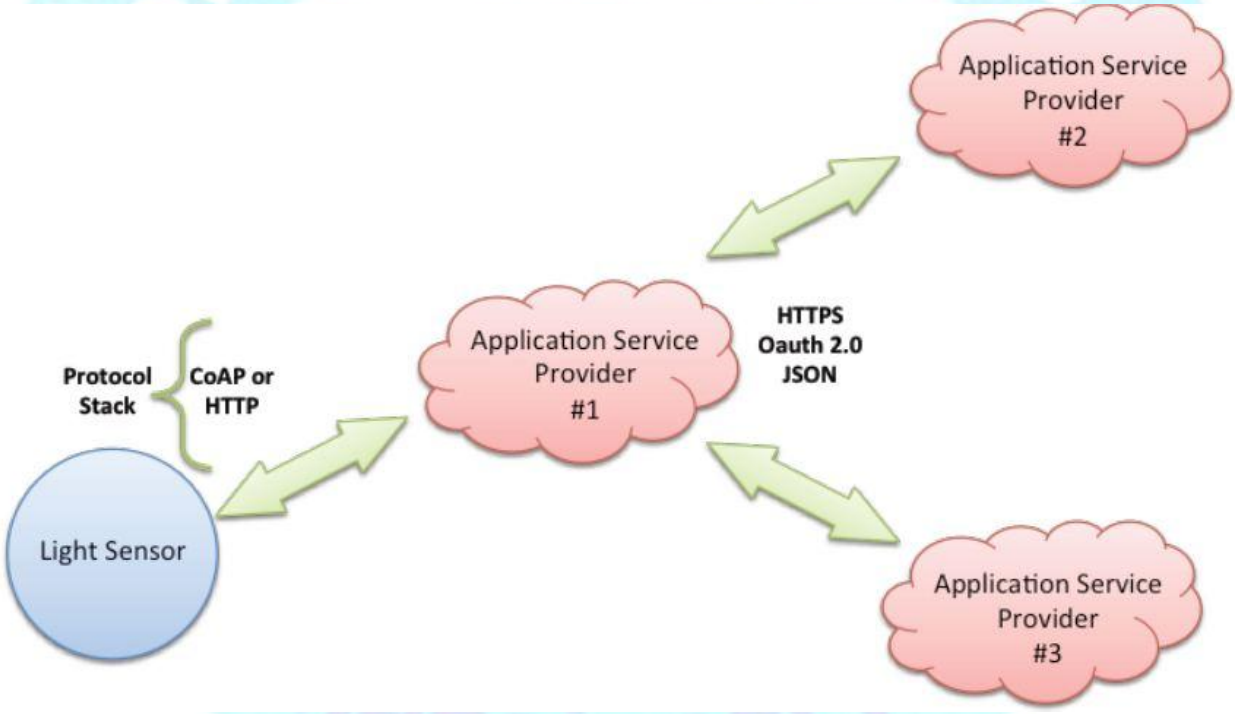

Fig 4: Back-end data sharing model diagram

IoT-Applications

IOT applications are used widely in many domains. Healthcare, agriculture, smart buildings (school, hospital, home) , supply chain management , Transportation and defense.

Agriculture

Internet of Things can be of great use in the field of agriculture. It can be helpful in monitoring growth of medicinal plants. These plants are fitted with RFID tags and sensors. When there is a drastic or unexpected change in the growth of plant due to temperature /humidity, the sensors sense this and the RFID (Radio Frequency Identification) tags send the EPC (Electronic Product code) (information) to the reader and are shared across the internet. The farmer or scientist can access this information from remote place and take necessary actions.

Smart Buildings – School

A school has many buildings in its campus like Administration block, library, Refreshment building, teaching block, etc. All these buildings have their own ventilation mechanism, ACsupply and elevator systems. These facilities have to be individually managed and maintained which becomes a tedious process. This scenario can be easily handled using Internet of Things for better management of the facilities. Each of the above blocks is fixed with RFIDtag that keeps monitoring the ventilation, AC supply behavior. The RFID system keeps sensing the change in environment and collects the data and sends it to the Information-gathering manager present in the respective block. Since the school campus will be equipped with Wi-Fi, the data from here is sent to the Central Control system. The control system on receiving the data will take necessary actions such as reducing the AC supply or stopping the elevator service. A communication mediator is required to mediate between the physical world and information world. Hence using IOT, steps are taken without human intervention.

Healthcare-Telemedicine

IOT plays a crucial role in healthcare. It can be used in many ways such as tracking the number of patients in a hospital, identifying the right patient for the right medicine and monitoring a patient's health conditions from a remote place which is known as Telemedicine. This includes providing treatment, diagnosis and treatment. Ambient assisted living provides technical systems for elderly people who are alone at home and need to be monitored. The patient's health status is periodically sensed using RFID and sensors. The doctor from a remote location provides medical assistance based on the information received.

CHALLENGES IN IOT

Though IOT has been a boon in many ways, it also poses certain challenges. The main challenges are privacy, reliability, data confidentiality and security. A vehicle attached withRFID tag leads to lack of privacy for the passenger in the vehicle. IOT in healthcare can also lead to dangerous consequences such as the data present in the health status can be changed by an intruder , hence giving the doctor wrong information. Wireless sensors in war fields, if found by the enemies can be mishandled to generate false information. An individual's rightto privacy should be protected. Strong security and sound privacy solutions will lead to better acceptance by public. There should be laws and policies to curb the misuse of InTechnology. Global Standards need to be developed for the spread of this new technology.
There are many other technology challenges in internet of things as follows:

Device management: The number of sensors, gateways and devices will be extremely large and they are going to be spread over large geographical areas – often in remote, inaccessible and/or private locations. Ensuring that devices are completely automated and remotely manageable is a challenge.
Device diversity and interoperability: Take the example of a power network in a city, which Is sensor enabled, and needs to be monitored continuously in near real-time. The generation, transmission, and distribution functions in such a complex network require different types of sensor devices from different

vendors. As many vendors do not support any standards in their products, there are sure to be interoperability issues.

Integration of data from multiple sources: As you deploy an IoT application, you will get streams of data from different sources such as sensors, contextual data from mobile device information, and social network feeds and other web resources. It is important to note that the semantics of the data must be part of the data itself and not locked up within the application logic in different application silos.

Scale, data volume, and performance: Prepare your business to manage the scale, data volume, and velocity of IoT applications. As the number of users and devices scale, so will the amount of data that needs to be ingested, stored, and analyzed. You will have a Big Data problem on your hands, and standard architectures and platforms may be inadequate. Also, where stringent real-time performance is required, network and application level latencies may be a problem.

Flexibility and evolution of applications: You will witness sensors and devices evolving with new and improved capabilities. This will result in creation of new analytics techniques and algorithms, and new use cases and business models. You will need to quickly develop apps with minimal effort. You will need ecosystems and platforms that enable and sustain this.

Data privacy: A good bit of data collected from devices will be sensitive personal data that must be protected from unauthorized access and used only for the specific purpose for which the user has allowed that data to be collected. Users have to be provided with necessary tools that enable them to define the policies for sharing their personal data with authorized persons and applications.

Another challenge, though not a technological one, is that you will have to work with a number of stakeholders. IoT works in a complex ecosystem, and an end-to-end IoT application touches several technologies, engineering activities, and other entities. Your maturity as a collaborative player becomes significant, as you need to work with different types of entities and organizations such as silicon chipset vendors, embedded boards and device vendors, IoT platform providers, communication service providers, system integrators, app developers, industry alliances as well as niche technology companies and startups.

CONCLUSION

Internet of things is a new internet application which leads to an era of smart technology where there exists thing-thing communication rather than human-human communication. Through IOT, each and every object in this world can be identified, connected and take decisions independently. Wireless sensor networks and embedded systems play an important role in developing IoT Applications. Just as the internet has transformed businesses and lifestyles in the last twenty years, IoT will disrupt your organization's relationship with its stakeholders. While it is complex, and poses some risks and is still evolving, many pioneers have started adopting this technology. There are many privacy and security issues that need to be addressed. If these issues are addressed, then Internet of Things will definitely be the global mantra.

REFERENCES

[1]Yinghui Huang, Guanyu Li,"**Descriptive Models for Internet of Things"**, International Conference on Intelligent Control and Information Processing, August, 2010 - Dalian, China.

[2] Daqiang Zhang, Laurence T. Yang, Hongyu Huang, "**Searching in Internet of Things: Vision and Challenges**", Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications, 2011.

[3] Yinghui Huang, Guanyu Li "**A Semantic Analysis for Internet of Things**" , International Conference on Intelligent Computation Technology and Automation , 2010.

[4] Lu Tan, Neng Wang, "**Future Internet: The Internet of Things**", 3rd International

Conference on Advanced Computer Theory and Engineering (ICACTE) , 2010.
[5] Louis Coetzee, Johan Eksteen , "**The Internet of Things – Promise for the Future? An Introduction ",** IST-Africa 2011 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, ISBN: 978-1-905824-24-3, 2011.
[6] COY, P. and GROSS, N. et al. *21 Ideas for the 21st Century*. Business Week Online, 1999, pp. 78-167. Available from: http://www.businessweek.com/1999/99_35/2121_content.htm
[7] NI, L.M. *China's national research project on wireless sensor networks*. Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'08), 2008, p. 19.
[8] HATLER, M., GURGANIOUS, D. and CHI, C. *Industrial wireless sensor networks. A market dynamics report*. ON World, 2012.
[9] Figure courtesy of Silicon Labs and RTC Magazine: http://rtcmagazine.com/fi les/images/4151/ RTC1212_SilLabs_fi g1_medium.jpg
[10] Yole Development SA. *MEMS technology: World's smallest barometric pressure sensor*. Micro News, 2009,78:1.
[11] KAHN, J. M., KATZ, R. H. and PISTER, K. S. J. *Mobile Networking for Smart Dust*. ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 99), Seattle, WA, August 17-19, 1999.
[12] ANG, R.J., TAN, Y.K. and PANDA, S.K. *Energy harvesting for autonomous wind sensor in remote area*. 33rd Annual IEEE Conference of Industrial Electronics Society (IECON'07), Taipei, Taiwan, 2007.
[13] TANG, L. and GUY C. *Radio frequency energy harvesting in wireless sensor networks*. International conference on communications and mobile computing, 2009, pp. 644648.
[14] Courtesy of Shenyang Institute of Automation, Shenyang, China, 2014.
[15] FP7 EXALTED consortium, *D3.3 – Final report on LTE-M algorithms and procedures*, project report, July 2012. Available from: http://www.ict-exalted.eu/fi leadmin/documents/EXALTED_WP3_D3.3_ v1.0.pdf76
[16] IEEE 802.15.4e-2012, *IEEE Standard for local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer*.
[17] IEEE Std 802.11™-2012, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifi cations*, IEEE Computer Society, March 2012.
[18] UIMER, C. *Wireless Sensor Networks*. Georgia Institute of Technology, 2000. Available from: www. craigulmer.com/portfolio/unlocked/000919_sensorsimii/wireless_sensor_networks.ppt
[19] PISTER, K. and DOHERTY, L. *TSMP: Time synchronized mesh protocol*. [C]. Proceedings of the IASTED International Symposium, Distributed Sensor Networks (DSN 2008), 2008, pp. 391398. Available from: http://robotics.eecs.berkeley.edu/~pister/publications/2008/TSMP%20DSN08.pdf
[20] SHELBY, Z. and BORMANN C. *6LoWPAN: The wireless embedded Internet*. New York, NY, USA: John Wiley & Sons Ltd, 2009. Available from: http://elektro.upi.edu/pustaka.elektro/Wireless%20 Sensor%20Network/6LoWPAN.pdf