Article can be accessed online at http://www.publishingindia.com

Internet of Things The Next Frontier of a Networked Community

Ninad Jadhav

Principal Architect, Tech Mahindra Ltd. Sharada Center, Erandwane, Pune, Maharashtra. India.
E-mail: ninadj@techmahindra.com

Abstract

The 'Internet of Things (IoT)' refers to the connected world of 'Things', often driven by intelligence, using information and communication technologies (ICT) and providing services to the society. 'Things' are not just an object of the physical world (physical things e.g. sensors, devices etc), but it could also represent objects of the information world (virtual things), which are capable of being identified and integrated into communication networks. In the world of 'Internet of Things' ordinary common place objects would have the ability to connect and communicate with other objects, people and systems. The 'Things' and the controlling processes would be able to analyze information and perform actions as well. 'This amalgamation of devices, software, communication and data would provide unforeseen services to the connected world. This technology is expected to bring benefits in various disciplines such as logistics, energy management, education, agriculture, health care, etc. Service providers have already started to offer IoT services for niche segments such as automotive, energy, utilities, transport, logistics and retail. However, IoT standards are still evolving and there are many challenges that need to be overcome before wide spread global adoption can be seen.

This paper provides an overview of the 'Internet of Things' covering aspects such as, the key facets of IoT, representative architecture, worldwide focus on IoT, market adoption and the future of IoT.

Keywords: M2M, Smart Objects, Internet of Things, IoT, IoE

1. Introduction

The term "Internet" refers to the interconnection of computer networks globally using the Internet protocol suite (TCP/IP). This inter-networking of computers is used to deliver a variety of services such as World Wide Web (WWW) services, files sharing, internet radio etc. The initiation of services is typically driven by humans through networked computers or by computers themselves and the services are typically serviced by networked computers. When machines utilize the network for communicating with remote machines or applications for the purpose of realizing some service, it is typically refered to as machine to machine (M2M) communication. M2M communication need not necessarily be over the Internet, but may also use varied networking technologies such as cellular, Bluetooth, Zigbee etc. Advances in embedded systems and miniaturization have made it possible for common place physical objects to have computing & communication capabilities and these are termed as 'smart' objects. When such 'smart' objects start to connect over the network and communicate with other objects, people or systems by augmenting such interactions with contextual information such as time, location etc. and exhibit 'intelligent' decision making, the machine to machine communication evolves in to the 'Internet of Things' (IoT).

2. IoT Landscape

Many different terms have been used to refer to the concept of 'The Internet of Things'. Physical Internet, Ubiquitous Computing, Ambient Intelligence, Machine to Machine (M2M), Web of Things, Internet of Everything (IoE) and Pervasive Internet are few of those. In general, these refer to Intelligent Systems involving 'Smart' objects that are connected to each other over some communication mechanism and cater to some service in coordination with humans and machines.

The below table lists some of the services where principles of IoT are applied.

Table 1: Sample IoT Services

Service Category	*Service Examples*
Smart Cities	Monitoring of parking spaces availability in the parking area. Intelligent and environment aware street lighting.
Smart Metering	Energy consumption, monitoring and management.
Security	Detection of gas levels and leakages in industrial environments.
Retail	Supply chain management – tracking supplies and storage.
Smart Homes	Home automation – video surveillance, light control etc.
Smart Cars	Connected vehicle - self diagnosis, car-to-car communication etc.
Healthcare	Health Monitoring – tracking and communicating vital health parameters.

IoT is an interdisciplinary domain involving sensors, devices, network, power etc. Realizing the concept of IoT requires considerations such as the overall architecture, communication technologies, security and privacy aspects, etc. There is a strong focus from standardization bodies in making this happen. Organizations such as ITU-T [13], IETF [12] and ETSI [5] are driving activities for standards development and coordination for M2M / IoT.

The academic institutes have a lot of focus on IoT too. e.g. The Auto-ID Labs [2], which comprises of seven of the world's most renowned research universities, is leading global network of academic research laboratories in the field of networked RFID.

There is a strong global focus on IoT including those from private and public parties. Chip vendors are making smart chips and providing application-level connectivity frameworks [10]. Software vendors are developing software platforms [16] designed to build and run the applications of the connected world. Service providers [1] are investing in facilities to accelerate the development of new applications for M2M and IoT. There is a strong verticalized industry specific focus as well [11]. Hardware and software vendors are collaborating for developing IoT solutions [4].

Besides, regional organizations are also working to harness the promise of IoT. e.g. the IoT European Research Cluster (IERC) is trying to address the large potential for IoT-based capabilities in Europe and to coordinate the convergence of ongoing activities [6]. Governments have also realized the need to address M2M / IoT. e.g. The Government of India has actively started to pursue preparation of policies around M2M / IoT communications [9] and has setup a task force for addressing M2M in the country. In its 2014-15 budget, the Indian Government has announced a sum of Rs.7060 crore in the current fiscal for the project of developing "One Hundred Smart Cities" [17].

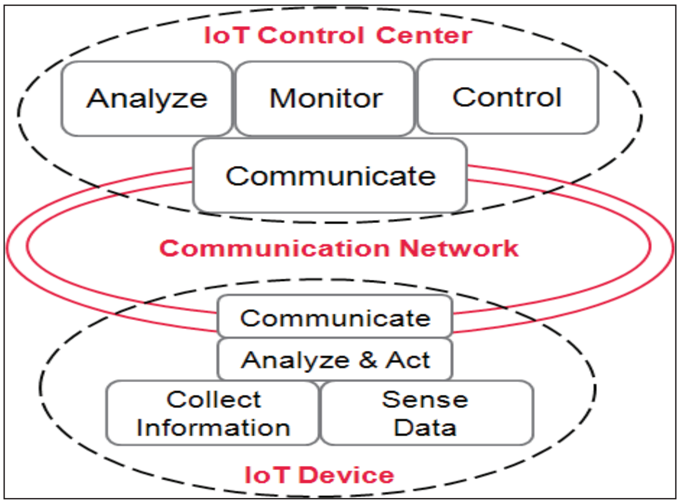
According to a analysis report [18] [3] there has been an broad interest in M2M solutions across 5 key M2M sectors including Automotive, Energy and utilities, Transport and Logistics, Manufacturing / Consumer electronics and Consumer goods / Retail. According to a leading M2M service provider who is serving around 7.8 million M2M connections globally [19], an increasing number of global businesses are incorporating M2M communications into their core operations, leading to greater productivity, enhanced customer service, lower energy use and decreased carbon dioxide emissions.

In summary, there is a strong drive towards IoT from standardization bodies, academia, device vendors and service providers. Service providers have identified IoT as a key driver for the enhancements of the communication network leading to efforts such as 4G & beyond and device to device communications. Overall, industry specific solutions, expanding communication networks, economics of scale of IoT enabled devices and viable business benefit propositions will lead to better adoption of IoT.

3. Key Aspects of IoT

Key elements of the IoT system are intelligent devices & the controlling entity. The figure below provides a logical representation of the IoT eco-system.

Figure 1: IoT Eco-system



Sensing & Collection of Information: The IoT devices should be able to collect or sense information based on their specific capability. e.g. a light bulb will sense the ambient light in the environment. Sensors could be of any kind - wearable, ingestible, implantable! e.g. a Smart watch or a wearable wireless accelerometer to measure daily exercise progress, an ingestible biomedical sensor that can be administered with pills or incorporated into medicines to measure vital signs for the patient, an implantable pressure sensor that can measure pressure etc.

Analysis and Act Upon the Information: The information collected by the object has to be analyzed and acted upon. A sensing and actuating device may detect or measure information related to the surrounding environment and convert it into digital electronic signals. It may also convert digital electronic signals from the information networks into operations. e.g. a plant sensor determines the moisture in the soil periodically and when it finds that the moisture level in the soil has dropped it decides to send a SMS to the controlling system. Similarly, devices should be capable of executing operations based on information received from the control systems. e.g. a water pump is instructed to start or stop water flow based on the need of water.

Communication of Information: The devices should have capability to communicate information over some communication network. Based on the device capability it could communicate through various mechanisms such as the cellular network, device to device communication technologies such as Bluetooth or Zigbee, or directly over the IP network.

Analysis, Monitoring, Control & Management: Backend systems should have the capability to configure the devices, monitor them and control them. These systems should also be able to receive information from the devices, analyze it, take appropriate action and generate management dashboards.

Realization of an IoT service requires a lot of considerations. Some of the key ones are listed below.

Device Capabilities: Devices should have the capability of sensing, actuation, data capture, data storage and data processing. The specific need of device capabilities will differ from application to application.

Device Addressability: It is required that devices be locatable or addressable. e.g. by using a unique IPv6 address or mobile number.

Device Identification: Devices need to be uniquely identifiable to be able to determine the characteristics of the device for controlling and information collection.

Accessibility: The devices should be accessible over some communication mechanism or through other devices.

Security: Security is a key IoT concern. It is important to maintain confidentiality, authenticity and integrity of the data that is being communicated.

Privacy: Devices and services are associated with users. Data collected by the devices may contain information concerning their owners or users. Thus, it is required that the IoT service provides privacy protection during data communication, storage and processing.

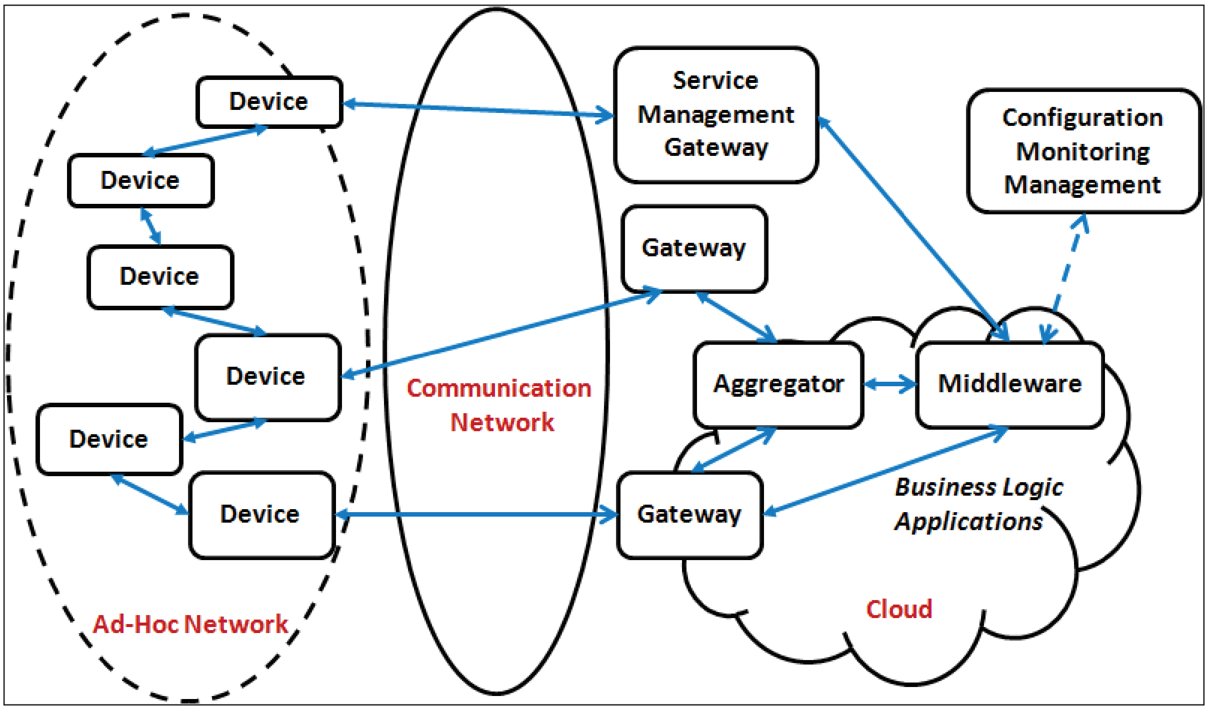
Policies: IoT applications are likely to generate a lot of traffic. It is important to define policies about data communication, alerts generation etc. and tune those based on the service requirements or traffic analysis.

Maintenance: Given that IoT services will result in a larger quantity of devices, it is going to be difficult to maintain those devices. Devices need to support some self diagnosis capabilities to alert the management system about its health.

4. IoT Architecture

The concept of IoT is still evolving and cannot be necessarily modeled in a uniform way. The below diagram provides a potential architectural model for implementation.

Figure 2: IoT Architecture



The devices communicate information to a Gateway that understands the communication protocol that the device uses. Due to existence of multiple communication mechanisms, there may be different types of gateways talking to the specific devices that understand the particular communication mechanism. Devices may communicate with other devices directly i.e. without using the communication network or through the communication network without a gateway as an intermediatory [14]. An aggregator may serve the function to provide a uniform view across multiple devices and gateways. The aggregator will have the capability to talk to multiple types of gateways and communicate in a uniform way to the Middleware which hosts the business logic of the specific service that is realized. The Middleware and its associated entities would have monitoring, management and control functions to overlook the IoT service. There may be other functions in the IoT eco-system based on the specific design of the IoT solution. e.g. for systems which depend on cellular communication, a separate service management function may exist which addresses the provisioning and activation of the Subscriber Identity Module (SIM). Some of the IoT eco-system components can be hosted in the Cloud environment.

5. An Example of Manifestation of IoT

As an illustration of IoT, consider a scenario where a forest needs to be tracked for illegal tree felling to avoid deforestation. Tracking device can be camouflaged and made to blend in with the trunks of trees. It would be difficult to provide cellular or wired networks for these devices in the forest. However, device to device communication technology could be used for these devices. The devices could potential connect with other devices and form an ad-hoc network of connectivity. When lumber gangs try to harvest a tagged tree, the device associated with the tree can start sending notification messages through this ad-hoc network to the control center (middleware) and thus notify the tree harvesting attempt in real-time to the law enforcement agencies. Furthermore the location capability of the devices would help the officials to track the felled trees being transported, intercept and arrest thieves in the act of selling wood. The Law enforcement agencies in Brazil implemented a similar solution in the rain forest of Brazil to track illegal tree felling [15].

6. Findings & Deliberations

Success of IoT depends on contribution from multiple entities of the IoT eco-system. Industry specific standards (e.g. health, manufacturing etc.) will have to evolve and reach a critical stage of wide adoption. Standardization bodies will play a key role in evolving such standards. One key element of the IoT systems is the IoT devices. Device manufacturers will have to ensure that the manufactured devices comply with international specifications and are interoperable with other elements in the IoT system. IoT offers tremendous potential for industries to benefit from, in terms of operational efficiencies, enhancing customer experience and delivering new services. e.g. the Railroad / Railways industry could use IoT sensors to keep track of the rail tracks to do preventive maintenance and avoid accidents due to issues with the rail tracks. An exporter of perishable items will be able to track the environmental conditions in which the goods are being transported, the state of the goods itself and the time to deliver, thus ensuring quality of service. The telecom service providers can play a pivotal role for such implementations. Communications between the devices and the backbone systems is a key aspect of IoT. Telcos could offer M2M based connectivity services required. They can further evolve as a M2M service providers to offer various M2M services to the industry and government organizations. e.g. Telecom service provider Vodafone provides M2M services and focused on solutions for major verticals like Utilities, Automotive, Manufacturing, Transportation & Logistics, and Financial Services sectors. An example of the verticalized service offering is its strategic partnership with Mahindra & Mahindra for providing M2M connectivity for 'e2o' (the Mahindra 'connected' car), to have telematics based features that enable 'anytime, anywhere connectivity' between consumer and their cars. Device conformance and quality test standards need to be evolved. Government agencies need to formulate national policies around M2M / IoT communications to further IoT. In addition, the governments should themselves adopt IoT and reap its benefits.

The IoT eco-systems need to be made plug and play to enable smooth scalability. e.g. when a device is deployed, the device should be able to detect communication networks available to it and other devices to communicate with. IoT services need to be relatively easy to use, which means that the ability to configure, control and monitor the IoT eco-system should be reasonably well defined. The system should be able to track the happenings in the IoT environment. e.g. logging interactions between devices and systems to be able to analyze as to who initiated a certain action and what was the trigger for that initiation. The devices need to have self diagnosis capabilities to be able to generate alerts upon certain conditions. e.g. low battery. Similarly, the system should be able to track device functioning – e.g. device not reachable. Mechanisms such as - password change alert, multiple accesses through a single log-in, alert when password not changed for a minimum duration – needs to be implemented to ensure security.

As the adoption of IoT picks up, it would lead to considerable increase in informational data. This data needs to be analyzed for generating actionable intelligence. e.g. data generated from monitoring of an industrial equipment may provide early diagnosis of potential failure of the equipment and this can be used to do preventive maintenance. However, the huge volume of data itself would require considerations for storage and Big Data analysis techniques for processing. Given the increase in consumption of video content by consumers, the cellular, and wireline networks of today are already falling short of supporting the bandwidth requirements. While the communication networks will continue to evolve, would they be sufficient to handle the additional IoT traffic data requirement is a question of considerable interest. Device to Device communication (D2D) could be a driver to offload backbone data traffic. D2D can be used for proximity-based IoT services and is already supported by several standards such as ZigBee, Bluetooth, NFC and WiFi-Direct. Currently, the 3GPP standardization body is working to extend this feature to the LTE networks.

However, there are still many challenges in the adoption of IoT. Cost of implementing an IoT solution is still a major concern. The overall solution cost makes a difficult business case. Enterprise's still don't see a major incentive in implementing IoT, as the perceived return on investment is not attractive compared to the state of current operations. Governments are pushing for a risk-reward model and suggesting a private public partnership model for rolling out IoT solution instead of upfront investments. For the end to end service providers this makes it very difficult to price their solution. Besides, there are societal implications in adopting IoT as well. Potential loss of employment is a concern in some market segments. Adoption of IoT is being enforced by authorities, but unless it is accepted in spirit it won't be effective. E.g. some local authorities have made it mandatory to implement school bus tracking system. Implementing only GPS tracking of the school bus will only help to certain extent in knowing the location of the bus at a given point in time, but unless the solution is used effectively to track other aspects such as bus halt time, activities in the bus through video recording etc, its effectiveness will not be fully realized.

7. Conclusion/Implications

While the realization of IoT services is a reality today, the adoption of it depends upon many factors. e.g. How do you make the system simple for the consumer to use? As organizations and individuals put their trust in IoT, how do you ensure that the system is not tampered with and affects business? How does the IoT system scale easily and yet remain manageable? How does one buy off the shelf IoT devices and get them to work with their IoT service? Addressing such needs requires considerable effort on part of the industry, academia and standardization bodies to work in close coordination.

Analysts predict that 'The Internet of Things' is evolving from a niche area into a mainstream activity, especially in the next three years and enterprises should seriously investigate and initiate pilot projects to position themselves to exploit the coming opportunities [7, 8]. Advances in communication technologies, electronic miniaturization, affordability of devices, communication & services and above all the benefits of connected world solutions is providing impetus for furthering of M2M / IoT. Real world applications of M2M/ IoT are in use today. The world has already started to witness commercialization of M2M / IoT solutions such as smart metering, energy monitoring, e-Health, intelligent transportation systems etc.

Much of IoT adoption today focuses on productivity and effciency gains. 'IoT' is being used as a suppliment for business-as-usual. However, the benfefits of IoT can be truly reaped, if it is treated to be a transformational and disruptive technology. It can be safely predicted that the drive towards developing intelligent IoT solutions and its adoption will only continue.

References

Additional AT & T Foundry Innovation Center Opens in Plano. (2013). Retrieved from http://www.att.com/gen/press-room?pid=24797&cdvn=news&newsarticleid=36994

AutoIDLabs. Retrieved from http://www.autoidlabs.org/

Beecham Research. (2012). Research Report commissioned by Oracle. *Designing an M2M platform for the connected world.*

Collaboration between Intel, McAfee and Wind River for IoT. Retrievd from http://www.intel.com/content/www/us/en/internet-of-things/videos/collaborating-for-the-internet-of-things.html

ETSI, Connected Things. Retrieved from http://www.etsi.org/technologies-clusters/clusters/connecting-things

European Research Cluster on the Internet of Things. Retrieved from http://www.internet-of-things-research.eu/

Gartner Analyst(s): David W. Cearley, Carl Claunch, 12 February 2013, "Gartner's 2013 The Top 10 Strategic Technology Trends for 2013", G00247453

Gartner Analyst(s): LeHong, H., & Fenn, J. (2013). *Hype cycle for emerging technologies*. G00252762.

Government of India, Ministry of Communications & IT, Department of Telecommunications, NT Cell, Minutes of Meeting, M2M Policy & Regulatory Committee meeting to form policy around "Machine to Machine communications. (2013, 5th August). Retrieved from http://dot.gov.in/sites/default/files/Minutes_of_M2M_policy_committee_Meeting_5_8.pdf

Internet of Everything Connection Manager, Qualcomm Developer Network,https://developer.qualcomm.com/mobile-development/mobile-technologies/internet-everything-connection-manager

Introducing the Industrial Internet, General Electric. Retrieved from http://www.ge.com/stories/industrial-internet

Ishaq, I., Carels, D., Teklemariam, G. K., Hoebeke, J., Abeele, F. V. D., Poorter, E. D., Moerman, I., & Demeester, P. (2013). IETF Standardization in the Field of the Internet of Things (IoT): A Survey. *Journal of Sensor and Actuator Networks*, ISSN 2224-2708.

ITU-T: Global Standards for the Internet of Things. Retrieved from http://www.itu.int/en/ITU-T/techwatch/Pages/internetofthings.aspx

ITU-T. (2012). Recommendation ITU-T Y.2060. *Overview of the Internet of things.*

Abdine, R. (2013). How M2M Technology is protecting Brazil's Amazon rainforest. *M2M Magazine*. Retrieved from http://www.machinetomachinemagazine.com/2013/01/17/how-m2m-technology-is-protecting-amazon-rainforest/

ThingWorx platform, http://www.thingworx.com/platform/

Union Budget (2014-2015). National Portal of India, Economic Initiatives, Smart Cities, Retrieved from http://india.gov.in/spotlight/union-budget-2014-2015

Vodafone, Circle Research, Analysys Mason, (2013). The M2M adoption barometer 2013. Report.

Vodafone Group Plc. (2012). *Annual Report.*