A Review of the Internet of Things

Naina Lohana, M. Mani Roja

Abstract: In this paper an effort is taken to review the concept of the Internet of Things (IoT). It has gained popularity in the recent years due to its wire-ranging applications. As the world moves towards a future with more and more devices linked to the Internet, this paper looks at the elements of IoT, its communication models, the challenges it faces and its applications.

Keywords: IoT

I. INTRODUCTION

The term 'Internet of Things (IoT)' was coined by Kevin Ashton at MIT in 1999. While there is no official definition for this term, it can be described as a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction [1].

The basic idea of this concept is the ubiquitous presence of elements like Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. - which, through unique identifiers, are able to interact with each other and achieve a common goal. The IoT concept will have a great impact on many aspects of everyday life and the behavior of potential users. Private users will benefit from IoT effects in domestic and working fields. Assisted living, e-health and enhanced learning are a few examples of possible application scenarios in which the new paradigm will play a leading role in the near future. For business users, the most obvious consequences will be visible in fields of automation and industrial manufacturing, logistics, business/process management, intelligent transportation of people and goods, among others [2,8]. According to Intel's report 'Rise of the Embedded Internet': "The Internet of things will involve a massive build out of connected devices and sensors woven into the fabric of our lives and businesses Devices deeply embedded in public and private places will recognize us and adapt to our requirements for comfort, safety, streamlined commerce, entertainment, education, resource conservation, operational efficiency and personal well-being."

II. ELEMENTS OF IOT

There are three main IoT components:

a) Hardware - which is made up of sensors, actuators and embedded communication hardware

b) Middleware – constitutes on demand storage and computing tools for data analytics and

c) Presentation - easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications.

A. Radio Frequency Identification (RFID)

RFID is one of the major developments in technology in the recent years and it uses microchips for wireless data communication. They are an efficient replacement for traditional barcodes as they act as an automatic identification for anything they are connected to. Commonly used are passive RFID tags, which are not battery powered and they use the power of the reader's interrogation signal instead to communicate the ID to the RFID reader. Due to this it has found many applications in retail and supply chain management. The applications can be found in transportation: replacement of tickets, registration stickers, and access control applications.

B. Wireless Sensor Networks (WSN)

Wireless sensors are miniature devices that are essentially low power integrated circuits that use wireless communication for remote sensing applications. They are becoming more prevalent because of their low cost and efficiency. These factors have led to development and implementation of sensor networks consisting of a large number of intelligent sensors, enabling the collection, processing, analysis and dissemination of valuable information, gathered in a variety of environments. Active RFID is nearly the same as the lower end WSN nodes with limited processing capability and storage. Sensor data are shared among sensor nodes and sent to a distributed or centralized system for analytics. The components that make up the WSN monitoring network include:

a) WSN hardware - Typically a node (WSN core hardware) contains sensor interfaces, processing units, transceiver units and power supply. Almost always, they comprise of multiple A/D converters for sensor interfacing and more modern sensor nodes have the ability to communicate using one frequency band making them more versatile.

b) WSN communication stack - The nodes are expected to be deployed in an adhoc manner for most applications. Designing an appropriate topology, routing and MAC layer is critical for scalability and longevity of the deployed network. Nodes in a WSN need to communicate among themselves to transmit data in single or multi-hop to a base station. Node dropouts, and consequent degraded network lifetimes, are frequent. The communication stack at the sink node should be able to interact with the outside world through the Internet to act as a gateway to the WSN subnet and the Internet.

c) WSN Middleware - A mechanism to combine cyber infrastructure with a Service Oriented Architecture (SOA) and sensor networks to provide access to heterogeneous sensor

Revised Version Manuscript Received on October 28, 2016.

Naina Lohana, Department of Electronics and Telecommunication, Thadomal Shahani Engineering College, Bandra, Mumbai (Maharashtra)-400050, India.

Dr. M. Mani Roja, Department of Electronics and Telecommunication, Thadomal Shahani Engineering College, Bandra, Mumbai (Maharashtra)-400050, India.

resources in a deployment independent manner. This is based on the idea of isolating resources that can be used by several applications. A platform independent middleware for developing sensor applications is required, such as an Open Sensor Web Architecture (OSWA). The Open Geospatial Consortium (OGC) builds OSWA upon a uniform set of operations and standard data representations as defined in the Sensor Web Enablement Method (SWE).

d) Secure Data aggregation - An efficient and secure data aggregation method is required for extending the lifetime of the network as well as ensuring reliable data collected from sensors. As node failures are a common characteristic of WSNs, the network topology should have the capability to heal itself. Ensuring security is critical as the system is automatically linked to actuators and protecting the systems from intruders becomes very important.

C. Addressing schemes

The ability to uniquely identify 'things' is critical for the success of IoT. The few most critical features of creating a unique address are: uniqueness, reliability, persistence and scalability.

Every element that is already connected and those that are going to be connected must be identified by their unique identification, location and functionalities. The current Internet Protocol version 4 (IPv4) may support to an extent where a group of cohabiting sensor devices can be identified geographically, but not individually. The Internet Mobility attributes in the Internet Protocol version 6 (IPV6) may alleviate some of the device identification problems; however, the heterogeneous nature of wireless nodes, variable data types, concurrent operations and confluence of data from devices exacerbates the problem further.

Persistent network functioning to channel the data traffic ubiquitously and relentlessly is another aspect of IoT. Although, the TCP/IP takes care of this mechanism by routing in a more reliable and efficient way, from source to destination, the IoT faces a bottleneck at the interface between the gateway and wireless sensor devices. Furthermore, the scalability of the device address of the existing network must be sustainable. The addition of networks and devices must not hamper the performance of the network, the functioning of the devices, the reliability of the data over the network or the effective use of the devices from the user interface.

To address these issues, the Uniform Resource Name (URN) system is considered fundamental for the development of IoT. URN creates replicas of the resources that can be accessed through the URL. With large amounts of spatial data being gathered, it is often quite important to take advantage of the benefits of metadata for transferring the information from a database to the user via the Internet. IPv6 also gives a very good option to access the resources uniquely and remotely. Another critical development in addressing is the development of a lightweight IPv6 that will enable addressing home appliances uniquely.

D. Data storage and analytics

One of the most important outcomes of this emerging field is the creation of an unprecedented amount of data. Storage, ownership and expiry of the data become critical issues. The Internet consumes up to 5% of the total energy generated today and with these types of demands, it is sure to go up even further. Hence, data centers that run on harvested energy and are centralized will ensure energy efficiency as well as reliability. The data have to be stored and used intelligently for smart monitoring and actuation. It is important to develop artificial intelligence algorithms that could be centralized or distributed based on the need.

E. Visualization

Visualization is critical for an IoT application as this allows interaction of the user with the environment. With recent advances in touch screen technologies, use of smart tablets and phones has become very intuitive. For a layperson to fully benefit from the IoT revolution, attractive and easy to understand visualization has to be created. As we move from 2D to 3D screens, more information can be provided in meaningful ways for consumers. This will also enable policy makers to convert data into knowledge, which is critical in fast decision making. Extraction of meaningful information from raw data is non-trivial. This encompasses both event detection and visualization of the associated raw and modeled data, with information represented according to the needs of the end-user [3].

III. COMMUNICATION MODELS OF IOT

In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart object that outlines a framework of four common communication models used by IoT devices.

A. Device to Device Communication Model

The device-to-device communication model represents two or more devices that 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. Often, however these devices use protocols like Bluetooth, Z-Wave, or Zig Bee to establish direct device-to-device communications as shown in Figure 1. 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 IoT 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.

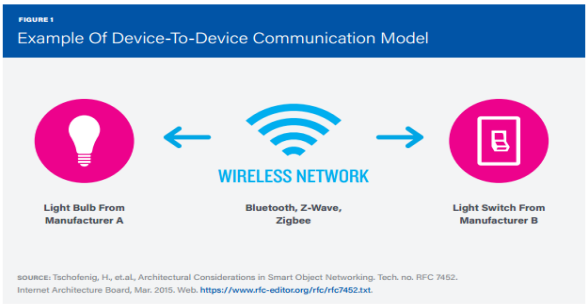

Figure 1: Device to device communication model [4]

From the user's point of view, this often means that underlying device-to-device communication protocols are not compatible, forcing the user to select a family of devices that employ a common protocol. For example, the family of devices using the Z-Wave protocol is not natively compatible with the ZigBee family of devices. While these incompatibilities limit user choice to devices within a particular protocol family, the user benefits from knowing that products within a particular family tend to communicate well.

B. Device to Cloud Communication Model

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, as shown in Figure 2. An example of cellular-based Device-to-Cloud would be a smart tag that tracks your dog while you're not around, which would need wide-area cellular communication because you wouldn't know where the dog might be.

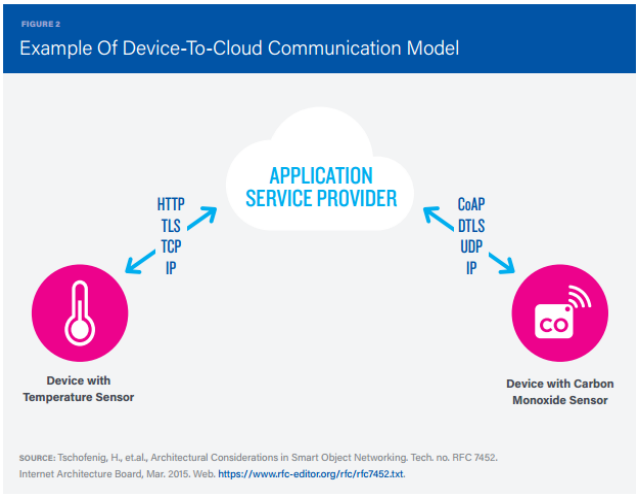

Figure 2: Device to Cloud Communication Model [4]

However, interoperability challenges can arise when attempting to integrate devices made by different manufacturers. Frequently, the device and cloud service are from the same vendor. 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. This is commonly referred to as "vendor lock-in'', a term that encompasses other facets of the relationship with the provider such as ownership of and access to the data. At the same time, users can generally have confidence that devices designed for the specific platform can be integrated.

C. Device to Gateway Communication Model

In the device-to-gateway model, or more typically, the device-to-application-layer gateway (ALG) model, the IoT 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, as shown in Figure 3. Several forms of this model are found in consumer devices. In many cases, the local gateway device is a 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.

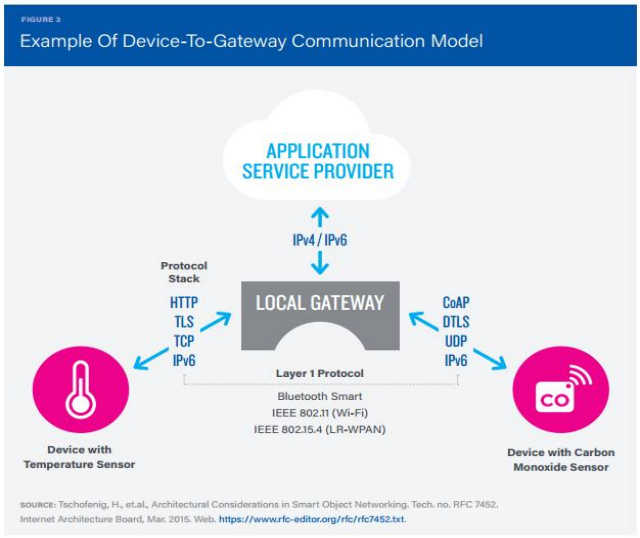

Figure 3: Device to Gateway Communication Model [4]

D. 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 [user's] 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 "IoT 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. For example, a corporate user in charge of an office complex would be interested in consolidating and analyzing the energy consumption and utilities data produced by all the IoT sensors and Internet-enabled utility systems on the premises. Often in the single device-to-cloud model, the data each IoT sensor or system produces sits in a stand-alone data silo. An effective back-end data sharing architecture would allow the company to easily access and analyze the data in the cloud produced by the

whole spectrum of devices in the building. Also, this kind of architecture facilitates data portability needs. Effective back-end data sharing architectures allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers.

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. A graphical representation of this design is shown in Figure 4 [4,5,7].

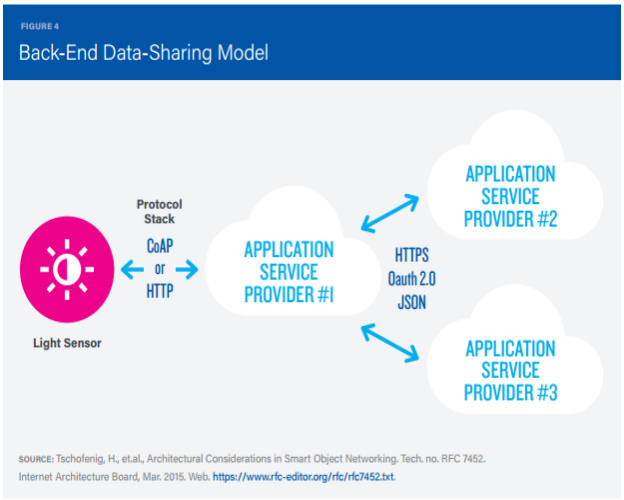

Figure 4: Back End Data Sharing Model [4]

IV. CHALLENGES FACED BY IOT

A. Security Issues

The overall security and resilience of the Internet of Things is a function of how security risks are assessed and managed. Security of a device is a function of the risk that a device will be compromised, the damage such compromise will cause, and the time and resources required to achieve a certain level of protection. If a user cannot tolerate a high degree of security risk as in the case of the operator of a traffic control System or person with an implanted, Internet-enabled medical device, then she may feel justified in spending a considerable amount of resources to protect the system or device from attack.

B. Privacy Considerations

Respect for privacy rights and expectations is integral to ensuring trust in the Internet, and it also impacts the ability of individuals to speak, connect, and choose in meaningful ways. These rights and expectations are sometimes framed in terms of ethical data handling, which emphasizes the importance of respecting an individual's expectations of privacy and the fair use of their data. The Internet of Things can challenge these traditional expectations of privacy.

C. Interoperability and standards

In the traditional Internet, interoperability is the most basic core value; the first requirement of Internet connectivity is that "connected" systems be able to "talk the same language" of protocols and encodings. In a fully interoperable environment, any IoT device would be able to connect to any other device or system and exchange information as desired. In practicality, interoperability is more complex. Interoperability among IoT devices and systems happens in varying degrees at different layers within the communications protocol stack between the devices.

D. Legal, regulatory and rights

The application of IoT devices poses a wide range of challenges and questions from a regulatory and legal perspective, which needs thoughtful consideration. In some cases, IoT devices create new legal and regulatory situations and concerns over civil rights that didn't exist prior to these devices. In other cases, these devices amplify legal issues that already existed. Further, technology is advancing much more rapidly than the associated policy and regulatory environments. Several potential regulatory and legal issues that affect the full spectrum of IoT applications.

E. Emerging Economy and Development Issues

The spread and impact of the Internet is global in nature, providing opportunity and benefits to developed and developing regions alike. At the same time, there are often unique challenges in developing regions related to the deployment, growth, implementation, and use of technology, including the Internet. It is reasonable to expect the same to be true for the potential benefits and challenges associated with the Internet of Things [4,6].

V. APPLICATIONS

Major applications of IoT include:

- **Smart home**

Smart Home or "Home automation" describes the connectivity inside our homes. It includes thermostats, smoke detectors, light bulbs, appliances, entertainment systems, windows, door locks, and much more. Popular companies include Nest, Apple, Philips, and Belkin.

- **Wearables**

Whether it is the Jawbone Up, the Fitbit Flex, or the Apple Watch – wearables make up a large part of the consumer facing Internet of Things applications.

- **Smart City**

Smart city spans a wide variety of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring. Smart City solutions promise to alleviate real pains of people living in cities these days. Like solving traffic congestion problems, reducing noise and pollution and helping to make cities safer.

- **Smart grids**

A future smart grid promises to use information about the behaviors of electricity suppliers and consumers in an automated fashion to improve the efficiency, reliability, and economics of electricity.

- **Industrial internet**

Many market researches such as Gartner or Cisco see the industrial Internet as the IoT concept with the highest overall potential. Applications among others include smart factories or connected industrial equipment. In 2014 GE reported roughly $1bn revenue with Industrial Internet products.

- **Connected car**

The battle is on for the car of the future. Whether it is self-driving or just driver-assisted: Connectivity with other cars, mapping services, or traffic control will play a part. Next generation in-car entertainment systems and remote monitoring are also interesting concepts to watch. And it is not only large automakers that play a role: Google, Microsoft, and Apple have all announced connected car platforms.

- **Connected Health**

The concept of a connected health care system and smart medical devices bears enormous potential, not just for companies also for the well-being of people in general: New kinds of real-time health monitoring and improved medical decision-making based on large sets of patient data are some of the envisioned benefits.

- **Smart retail**

Proximity-based advertising, In-store shopping behavior measurement and intelligent payment solutions are some of the IoT concepts of Smart Retail.

- **Smart supply chain**

Supply chains are getting smarter. Solutions for tracking goods while they are on the road, or getting suppliers to exchange inventory information are some of the Supply chain applications as part of the Internet of Things.

- **Smart farming**

The remoteness of farming operations and the large number of livestock that could be monitored makes farming an interesting case for the Internet of Things [3].

VI. CONCLUSION

Internet of Things is getting more prevalent as we move further in time and it going to be the basis of the future of technology. However there are some issues that need to be solved before any progress is made.

REFERENCES

1. M. Rouse Internet of Things. Retreived from http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
2. L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010
3. K. L. Lueth, IoT Basics: Getting Started with the Internet of Things, IoT Analytics(2015). Retrieved from https://iot-analytics.com/product/whitepaper-iot-basics-getting-started-with-the-internet-of-things/
4. K. Rose, S. Elridge, L. Chapin The Internet of Things: An Overview, Internet Society (2015). Retrieved from http://www.internetsociety.org/doc/iot-overview
5. D. Hamilton The Four Internet of Things Connectivity Models Explained. Retrieved from http://www.thewhir.com/web-hosting-news/the-four-internet-of-things-connectivity-models-explained
6. T.T. Mulani, S.V. Pingle Internet of Things, IRJMS Vol 2 Special Issue 1, March 2016.
7. B. Katole, M. Sivapala, V. Suresh,Principle Elements and Framework of Internet of Things, Research Inventy: IJES Vol 3 Issue 5, July 2013.
8. J. Gubbi, R. Buyya, S Marusic, M. Paluniswami, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions,Future Generation Computer Systems Vol.29 Issue 7, September 2013.