INTEROPERABILITY ISSUES IN IOT

4/8/2016

WHITEPAPER

Interoperability is the key issue ailing the mass adoption of IoT devices. Standardization is the remedy. This paper talks about the inherent Interoperability issues and the possible approaches to address them

Harsha Bagur, Technology Advisory

harsha@blrlabs.com

Interoperability Issues in IoT

WHITEPAPER

Introduction

Internet is considered as one of the most important and powerful creations in all of human history. Internet of Things (IoT), also known as Web of Things or Internet of Objects, represents the next wave of evolution that is promising to connect every object on earth; living as well as non-living. With this kind of a connectivity established, there is a possibility of generating and transmitting real-time data from all kind of objects -- homogeneous as well as heterogeneous, conveying all kind of statuses depending on the object to which this data is attributed to.

The data that is generated will pose a huge challenge, in terms of its assimilation and the derivation of the right context and meaning, by the receiving entities. There is, thus, a huge possibility of fragmentation in terms of technologies used to process this data. Moreover, numerous services and applications are bound to be developed to control and operate the connected things/objects. Hence, there is a strong need for a generic framework, which removes the fragmentation in technologies and provides for interoperability and ubiquitous access.

Building Blocks

Sensors and sensory nodes form one of the primary building blocks of the IoT. The type of sensors vary widely depending on the applications involved -- meters measuring the water levels, heat in a system, atmospheric temperature or a camera security system providing periodic images or live video. Each one of them will be associated with an object or be part of an object and each of them need to have a unique ID for addressing purposes. For the purposes of object tracking & identification in a retail environment, RFID and barcodes are the methods typically used for ID.

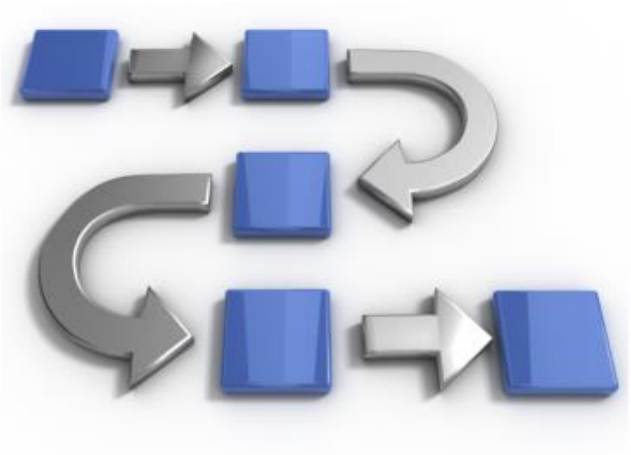
Smart Device, Edge Device	Connectivity	Aggregator, Hub	Remote Cloud based Processing
•Sensor – GPS, Proximity, Accelerometer, etc •Embedded Processing – Low Power, Low footprint •Standalone device	•Bluetooth (LE) •Wi-Fi •NFC •Zigbee, etc •Security, encryption	•A Gateway for connectivity •Aggregates the Sensor data and connects to the Cloud based storage •3G/4G	•Data Analytics for Business Intelligence •BigData

Typical components in the building blocks that make up the end-to-end IoT system is depicted above.

For specific usecases like the M2M (machine to machine) communication, the addressing as well as the communication mechanisms do vary. For two machines to communicate, the semantics have to pre-defined, accepted and programmed to be understood by each. This is where the standardization plays a key role. However, for certain M2M (machine to machine) communications and also those involving cloud connectivity & cloud centric interactions, IP is the mechanism typically used.

IoT comprises of multiple and heterogeneous building blocks and hence there is an inherent fragmentation in the system.

Integration and Interoperability



In any IoT scenario, the objects are all digital things connected to the internet. They are monitored and controlled through service frameworks and various applications -- custom as well as generic.

Consider a smart home scenario where all the lighting are connected and controlled through a web interface. An introduction of a new light bulb, from a different vender, should not alter the setup and create the need for a gateway for interoperability. Thus there is a strong need for standardization, that enables the semantics being conveyed and understood, and also to enable the interoperability of devices from multiple vendors.

Possible Approaches

Interoperability is needed at all levels. For a spatially distributed remote nodes setup (e.g. robotic control, industrial automation), wherein the processing capacities are low and power is a premium, the 6LowPAN is the preferred approach. These nodes, which are all homogeneous, will talk through a gateway, which in turns opens up these devices for accessibility from external world.

However in a Smart home network, we see a conglomeration of heterogeneous devices - ovens, dish washers, refrigerators, washing machines etc. These devices need, along with the device address, a kind of device type identification which is universal. The devices will all be connected to a smart gateway which paves way for internet access.

The devices in these kinds of scenarios need a Service discovery protocol which will ascertain the device capabilities. The preferred approach in this scenario is -- IP based addressing, a session layer based asynchronous hand-shaking protocol for service discovery & a CoAP/HTTP at application level. The gateways which are the primary access points should allow configurations and installation of applications.

In terms of building such models, we have most of the necessary tools/protocols available in the internet domain -- IP, TCP, CoAP, HTTP/S, etc.

However, the key need is standardization across vendors and a set of Open APIs for developers.

BLR LABS possesses the expertise in the areas of real-time embedded systems, which is critical for engineering low power, low footprint IoT edge devices

We also do possess the expert knowhow in connectivity protocols – BT, Wi-Fi, NFC etc which are critical for realizing the IoT usecases and for engineering end-to-end IoT scenarios

We have experienced professionals to address the custom needs in Cloud connectivity and Analytics

With the experience and expertise is possesses, BLR LABS aims to be the preferred partner in Architecting, Designing and Developing End-to-End Connectivity based Systems and Solutions to Consumer electronics, Telecom and IoT device makers & Software Providers