Towards a common definition and taxonomy of the Internet of Things

Contents

Introduction

The Internet of Things (IoT) topic has been receiving a lot of attention lately both from the commercial industry as well as research and education community. Most recently, large technology companies have initiated solution portfolios related to IoT, whether in full production or in beta, examples of those are Microsoft (http://www.microsoft.com/en-us/server-cloud/internet-of-things) , IBM (https://www.ibm.com/cloud-computing/bluemix/solutions/iot), Amazon (https://aws.amazon.com/iot) and Google (https://cloud.google.com/solutions/iot).

However, there is a confusion on what *Internet of Things* meaning is and there is an absence of a clear and agreed-upon definition across industry and research. The Internet2 community identified the urging need for a common definition through the numerous conversations around the topic part of the discussion in the Collaborative Innovation IoT Working Group (Internet of Things Collaborative Innovation Working Group, 2015). Moreover, the demand for a clear definition of the term extends beyond the commercial and research areas to the general public; a quick review of Google Trends for the term “Internet of Things” illustrates that there is an in increasing interest in looking up the definition of the term online (see Figure 1).

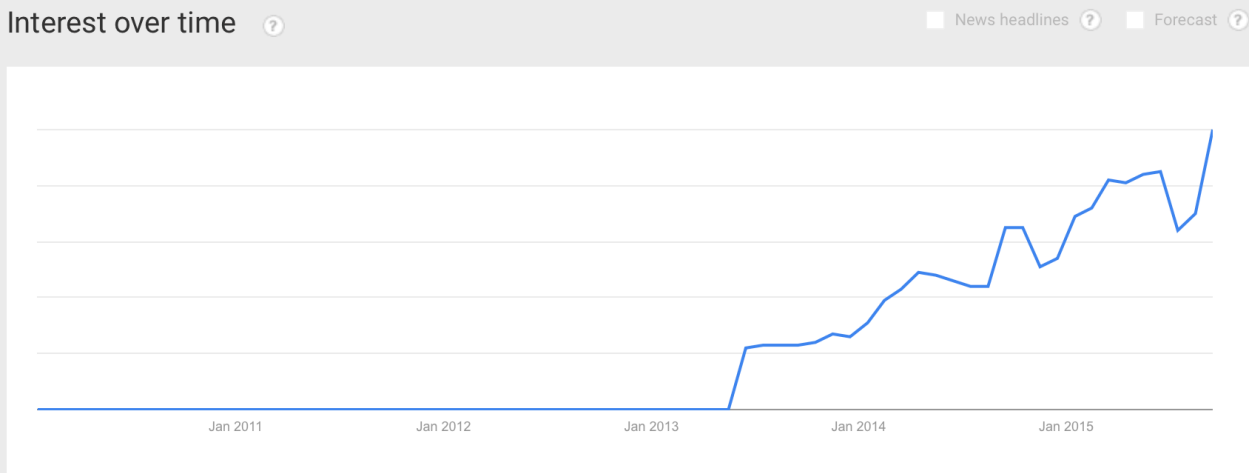


Figure 1 : Google Trends for "Internet of Things" October 2015

Some business research described IoT as physical assets equipped with sensors connected to information systems (An executive’s guide to the Internet of Things, 2015). Similarly, the National Science Foundation (NSF) launched a program that used Physical Connected Devices as an alternate, more straight forward reference to the IoT. National Institute of Standards and Technology (NIST) took the definition to a broader extend and introduced Cyber-Physical Systems program http://www.nist.gov/cps/. They further presented a draft of related definition,

published in the Cyber-Physical Systems Public Working Group (CPSPWG) as: “Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components”.

Forbes defined IoT as “connecting any device with an on and off switch to the Internet or each other’s) (A Simple Explanation Of 'The Internet Of Things', 2014).

Gartner’s definition for IoT is “network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment” (Internet of Things, IT Glossary, n.d.)

Where there is a generic and high level understanding of IoT and what it basically means. There is no consensus currently in the research or industry on a specific definition of IoT that covers all its characteristics and taxonomy.

In this paper we aim at introducing a universal definition for IoT that incorporates what is identified in the following sections as its main characteristics, taxonomy and domains and we also propose a preliminary maturity model and a foundation for a generic IoT stack and test bed.

Common characteristics of Internet of Things

Connectivity

One of the most common characteristics of IoT is that most physical devices, due to limited amount of storage and the need for a real-time stream of data, have a certain type of connectivity. The connectivity can be constant (sustained) or intermitted (occasional) and usually to a central end-point in which an aggregate of all streams of information provide the main repository of data for analysis.

Data Centric

The model of IoT involves the collection, transmission, and/or presentation of data. Sensors, evidently, collect readings from surroundings, and the possibilities of sensor readers is exceedingly increasing and to cover a broad range of use cases from health (e.g. heart rates, blood pressure, blood glucose level, insulting level…etc.) to environment (e.g. temperature, humidity, airflow, sound, motion, light…etc.) and including a variety of other types. IoT also transfer control data to physical devices to activate processes, switch circuit boards on, turn on motors or control other types of physical action.

Low power

Most devices used by IoT applications are portable, distributed, deployed outdoor, or movable [transportable] causing them to rely on battery power, solar, or Power over Ethernet (PoE). This feature is not unique to IoT but is distinctively prominent in the IoT realm and is impacting its emergence, development and deployment. It also creates one of its challenges although second to security.

Minimal Resources

A common characteristic of most IoT devices and applications is the limited resources used by the devices due to the restricted availability of power, network bandwidth and cost. Most IoT devices are small in size, use low powered CPUs, limited amount of storage and transfer small amount of data over slow connectivity (e.g. cellular, Bluetooth, ZigBee…etc.). Although some devices are more powerful and use much more resources, the majority of devices are build with minimum requirements of bandwidth and power.

Leveraging Cloud Services

Because of the widely distributed nature of the IoT devices and applications and the centralized connectivity requirements to bring sensor data back to a central data store in addition to the unpredictable resources utilization, cloud computing model provides a natural fit as an enabler for IoT, allowing connectivity, storage, management and analytics that are required for a successful implementation of IoT applications. This is demonstrated by the interest of most cloud computing service providers like Amazon AWS, Microsoft Azure and IBM BlueMix to offer IoT solutions which are integrated into their cloud offerings.

IoT Taxonomy

There is limited work on IoT taxonomy and most of the attempts are specific to industry solutions or market definition that is constantly dynamic. We identify the need for a generic, inclusive model for IoT taxonomy to defines not only its characteristics, development layers, use cases, and domains but also extends to become the foundation for building a usable IoT stack that assist in initiating or acceleration research, development and production in that area.

IoT Assurance Model

One of the main challenges facing IoT as identified by both Internet2 Collaborative Innovation Iot working group as well as End to End Trust and Security Working Group is *Security*. With the proliferation of devices, sensors and integrated applications, specifically in areas of health, financing and industrial monitoring/control, there has been a lack of standards for certain measures of encryption and authentication if any actually exist. Many of the protocols are not encrypted by nature and developer often opted for simplicity and time to market before security. In this paper we propose to use an assurance model, in which we provide a matrix of domains, use cases and contexts that assist developers and research to consider what security measures to incorporate in their work and to what level of assurance they adhere to and therefore offer to their users and stakeholders. The model, as depicted in figure 3, uses an axis for domains (e.g. sensor, local device storage, application, cloud services, data storage) and other for use cases (e.g. health, personal fitness, home automation…etc) and use auxiliary factors to provide contexts (like control, measurement or data transport) to present a general model for levels 1 through 6. Additionally, we suggest basic encryption and authentication measures for each level to warrant specific protection mechanisms to be incorporated in applications or production of IoT related elements (see Figure 2: IoT Assurance Model).

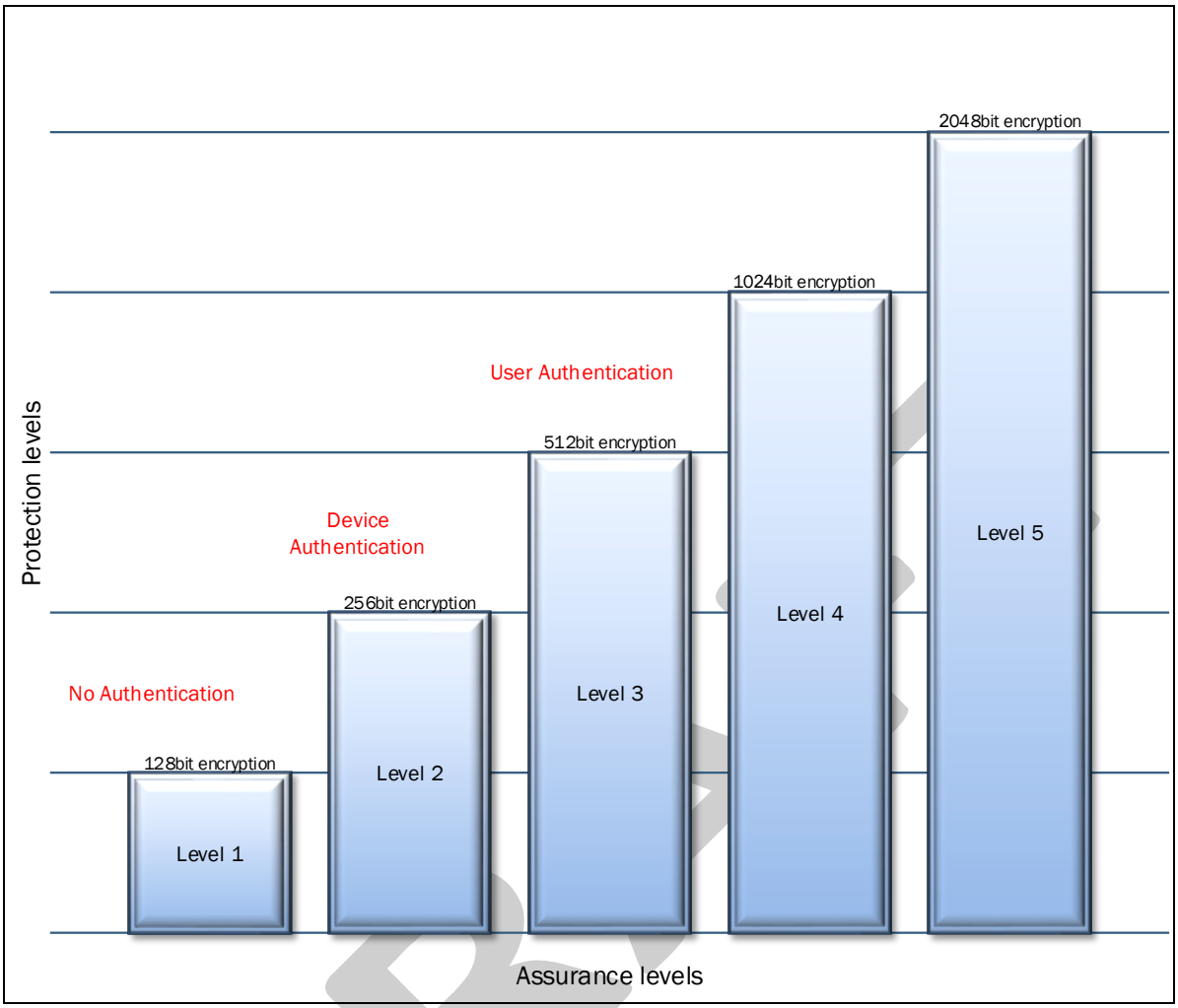


Figure 2: IoT Assurance Model

IoT Stack and Test Bed

Most development in the IoT arena include basic concepts and general framework that is become a common foundation for developers, here is a list of the main components of an IoT stack:

A Publish/subscribe model

Data communication and transfer between devices and application (endpoints) is typically done through an asynchronous operation with a publish & subscribe model in which endpoints "publish" message to "Topics" and other endpoints subscribe to the same topic to receive the messages. The relationships between the endpoints could be many-to-many or one-to-many and in both directions.

A light messaging protocol

Due to the characteristics and limitations of IoT devices and applications, communication between the end points is frequent and bandwidth availability and power is limited, thus and messaging protocol that is suited to such would be a light weight, low latency and reliable-but-simple messaging protocol. A REST API interface and JSON for data payload is a preferred style for communication and the two most appropriate protocols for IoT messaging are HTTP(s) and MQTT (MQTT, 2015). MQTT is designed with machine to machine connectivity in mind and leverage the "broker" approach to communication the messages and is ideal for light weight and small payload applications. Its simplicity is helping in promoting its use.

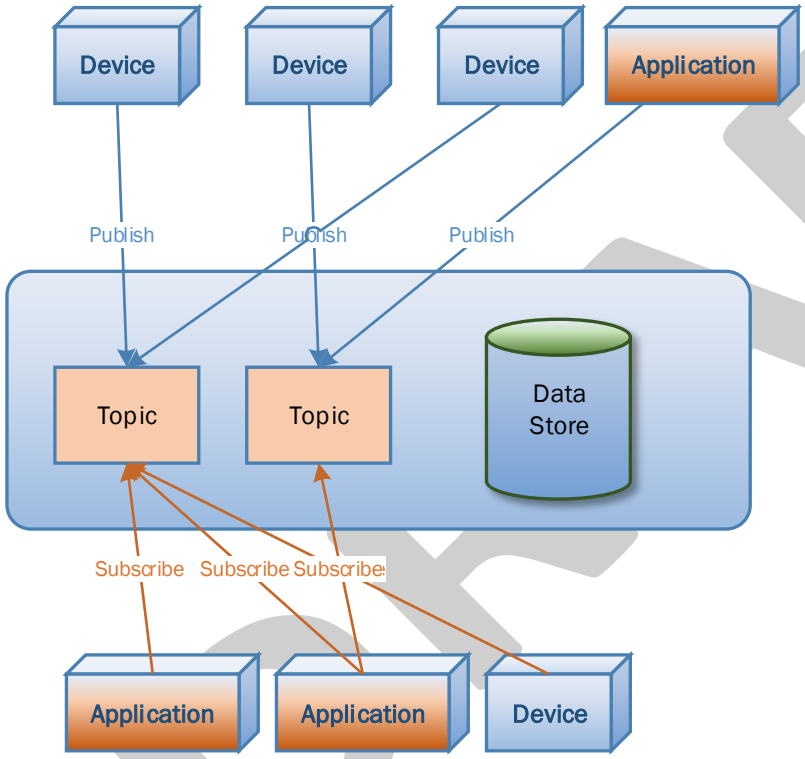


Figure 3: IoT Messaging diagram

Data Model

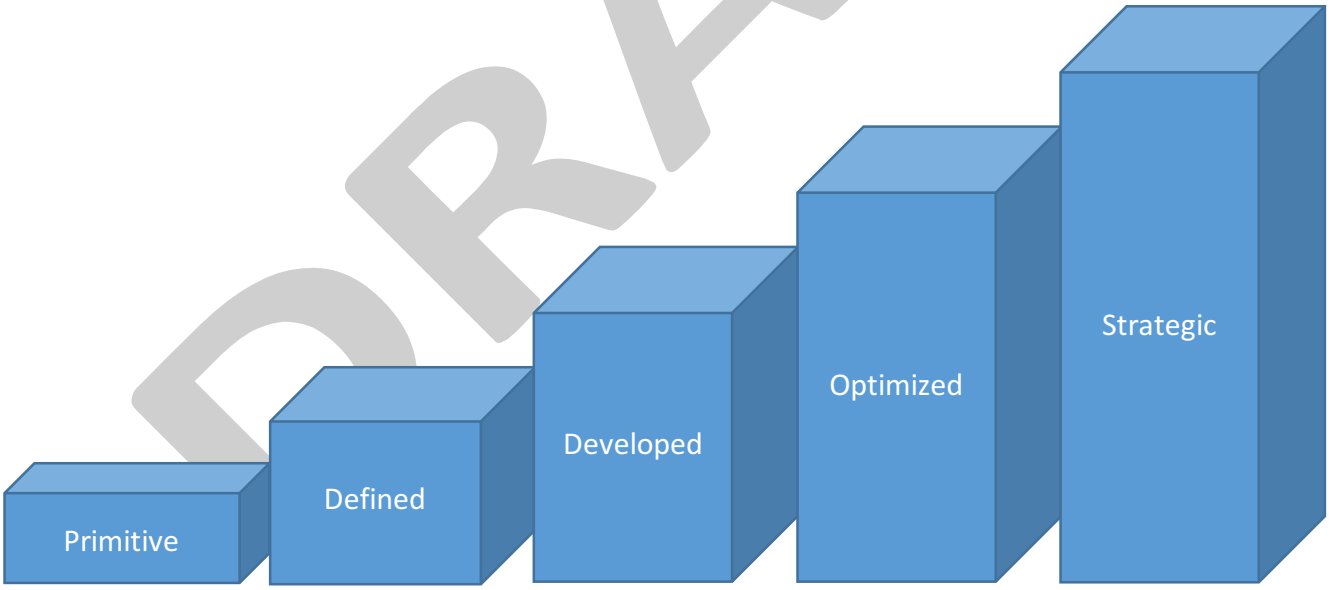
Data payload and stores are defined in a JSON style to represent attributes and values. JSON is lightweight, standardized and extensible which make it appropriate to represent the data structure sent or received by devices and applications.

Data Store

IoT use numerous type of data that is collected from sensors and applications which are stored in an unstructured way that makes NOSQL databases ideal for storage and retrieval of data by applications and endpoints. This facilitates the analytics and reporting against the data in real time or occasionally. Cloud NOSQL data stores are appropriate fit to store IoT data due to scalability and integration with online analytics tools

Iot Maturity Model

- **Device** (e.g. sensor) advancement in power utilization, computing power, (at rest) encryption capabilities and caching.
- **Infrastructure** (network connectivity, in transit encryption, reliability)
- **Data Analytics** (reporting capabilities, live-streaming analytics)
- **Usability** (user interface, ease of use, localization)
- **Management** (Asset management, configuration management)



Maturity Level 0 - Primitive

Maturity Level 1 – Defined

Maturity Level 2 – Developed

Maturity Level 3 – Optimized

Maturity Level 4 – Strategic

Closing remarks and call for actions