A presentation on IoT based on the book - “A Reference guide to the IoT”

Authored by Greg Dunko, Joydeep Misra, Josh Robertson and Tom Snyder ;RIoT, Bridgera

BY: MOHAMMED SHAHZAD

444105788@STUDENT.KSU.EDU.SA

Contents of the presentation

- Introduction to IoT
- Current applications in short
- Sections 1 to 5 from the book we are discussing about
- Concluding thoughts

Introduction

- IoT is the intersection of the digital with the physical.
- Physical devices are now enhanced with sensing, computing, and communication capabilities.
- Wearables such as Fitbit and connected home devices like Nest are most commonly cited examples of IoT.
- These are however quite basic early IoT systems.

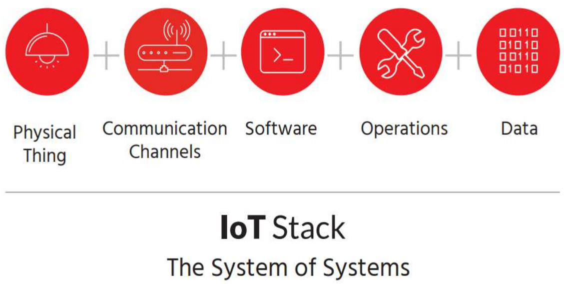
Applications of IoT

- Current and early IoT applications:

- IoT solutions are becoming popular at the city and county level to make emergency response services
- Smart home fire detector on the market warn people in cases such as fast moving tornadoes or forest fires.
- The basic wearable devices are connected to first responder systems as EMT's rush to an emergency.

Sections 1 through 5

- The book is divided into 5 sections.
- Section 1 deals with the **physical things** part of IoT.
- Section 2 is all about **communication** among IoT devices and between networks and "things"
- "The cloud" and other SaaS options and their Operations are discussed in section 3 and 4 respectively.
- Section 5 addresses data in IoT, concerns and "Big data"



Section 1: The Physical Things(1)

- Sensors and Actuators

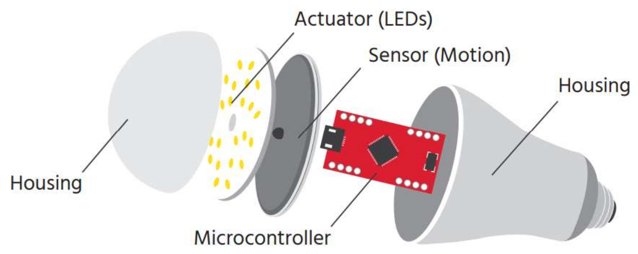
- The fundamental source of IoT data is sensors.
- A sensor (basically transducer) is a physical device that converts one form of energy into another. An actuator however takes an electrical input and turns it into physical action.
- One important characteristic of Sensors is it need to be accurate.
- since you will make mission-critical decisions based on later analysis of the data, which will hold little value if the data is wrong.

Figure: A temperature sensor module

Section 1: The Physical Things(2)

- Microcontroller: The “Brain” of the IoT Device.

- Specifications of the micro/controller device
  - -Microprocessor type(more memory or speed)
  - -Amount of memory
  - -operating voltage
  - -number and type of I/O ports
  - -control interface
  - -source of power(battery, mains electricity, solar)
- Battery size is a utility tradeoff in IoT devices

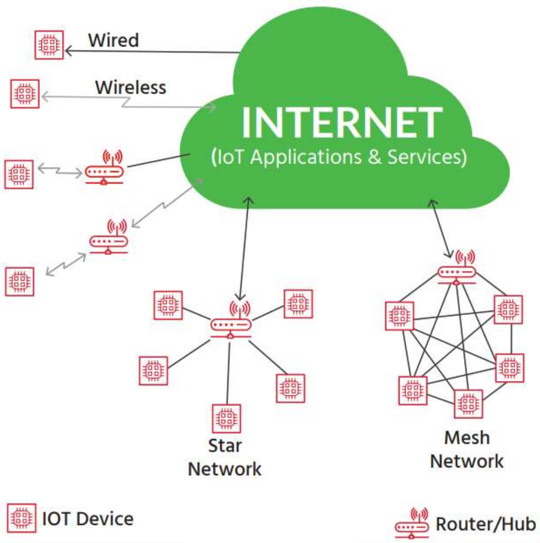


Anatomy of a **Thing**

Section 2: Communication channels(1)

- **Communication among things**:
  - Connecting things-to-things, things-to-server, server-to-server.
  - IoT systems enable Things to communicate with servers as well as other Things.

- **IoT Wireless Radio Solutions:**
- Your application will dictate the connectivity method needed for your device. Connectivity range options include:
  - - short range solutions (e.g. RFID or Bluetooth),
  - - medium range solutions (e.g. ZigBee, Thread, or Wi-Fi), and
  - - long range Wide Area Networks (WAN) solutions (e.g. cellular or satellite).



Types of **Node Architectures**

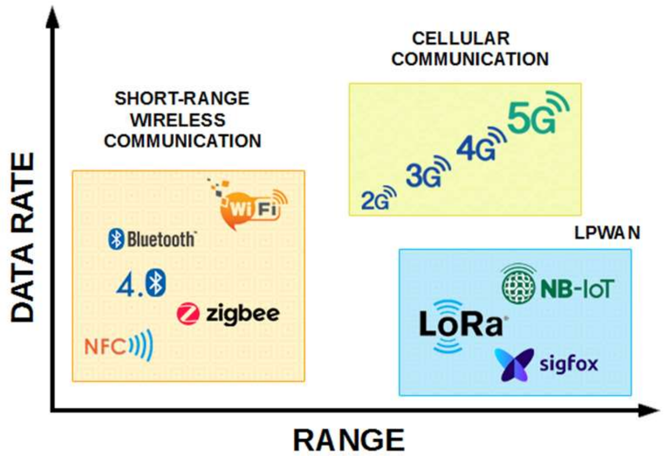
Section 2: Communication channels(2)

- 1) **Long Range IoT Radio Solutions:**

  Disadvantageous for:

  - Using cellular networks can be expensive. These networks are designed for voice and high data throughput/low latency communications, which are not typical requirements of IoT applications.
  - Cellular solutions are not designed for very low power operation.
  - older 2G and 3G infrastructure will likely begin to phase out.

- Instead of focusing on existing cellular technologies, we will introduce alternative long-range solutions.
  - Low Power Wide Area (LPWA) Networks
  - LoRa (LOng RAnge)
  - Sigfox
  - Satellite



Section 2: Communication channels(3)

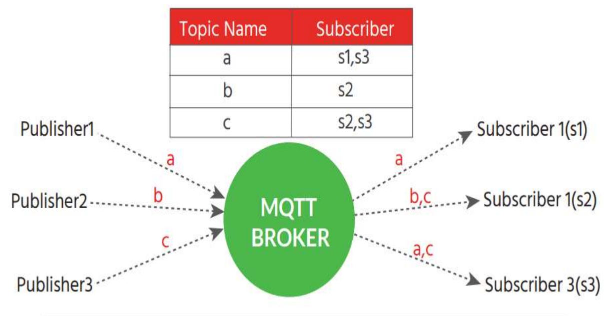
- 2) **Medium range IoT solutions:**
  - We define medium range as a radio solution with signal range no greater than 100 meters. Example: Zigbee, Wi-Fi, zwave.
- 3) **Short Range IoT Radio Solutions:**
  - We define short range as solutions with signal range ≤30m. The most common technologies in use include Bluetooth (or its evolution Bluetooth LE) and RFID.
- BLE Low energy Bluetooth is the hot topic for IoT services. One adv of Bluetooth is its user popularity, already integrated to mobile devices and low range.

Section 2: Communication channels(4)

- **Communication with the world**:
  - IoT systems enable Things to communicate with servers as well as other Things.
  - Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) are two alternative internet protocols. TCP/IP is power hungry.

- MQTT was originally used in satellite applications but has evolved to handle today's range of IoT applications.
- CoAP, on the other hand, is somewhat new and has been gaining traction.

- MQTT-MQTT uses a "publish/subscribe" message transport model.



Publish/Subscribe Model

Section 2: Communication channels(5)

- MQTT Advantages: independent operations, security, varied levels of QoS
- Disadvantages: need for central broker, TCP protocol implications like overhead.
- CoAP for "use with constrained nodes and constrained networks." Like MQTT, CoAP is commercially supported and growing rapidly among IoT providers.
- CoAP characteristics- UDP use, multicast, security with datagram protocol, web friendly.

Comparison of MQTT and CoAP protocals

MQTT	CoAP
Many-to Many communication protocol	One-to-One communication protocol
Synchronous or Asynchronous*	Asynchronous only*
Medium Level Security**	Medium Level Security**
More reliable message delivery than CoAP	Less reliable message delivery than MQTT
Scalability is easier due to pub/sub model	Scalability is more Complex
Simpler protocol spec may allow for simpler implementation	Easy translation to HTPP for simple web integration
No specified layout for data representation in a message	Provides inherent support for content negotiation and dynamic discovery
Does not support multicast operation	Supports multicast operation
Many software language content libraries	Many software language content libraries

* MQTT is most commonly run in Asynchronous only

** For higher-level security, other protocols such as Data Distribution Service (DDS) or Extensible Messageing and Presence Protocol (XMPP) should be considered.

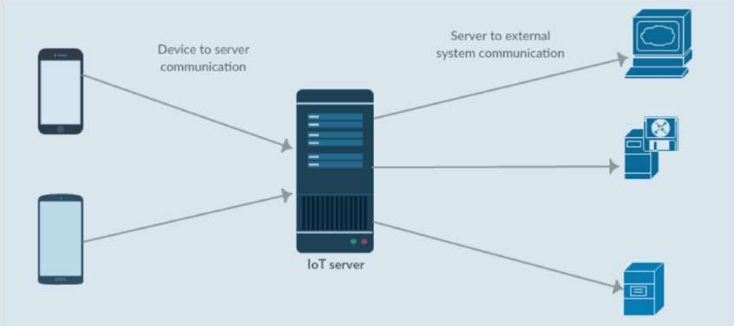
Section 2: Communication channels(6)

- **Reliability and Quality of Service**

- The amount of faults a system can sustain is called reliability, it includes:
  - Data reliability; because data can be tampered
  - Device reliability; because IoT devices can fail

- Data reliability depends on the accuracy of data collected and transmitted by the IoT system.

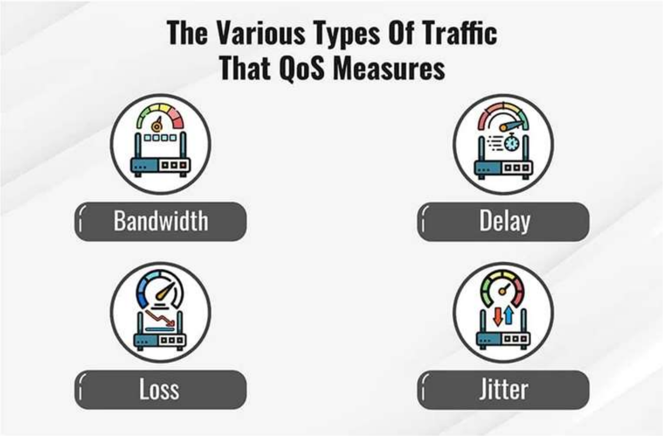
- Device reliability depends on largely on environmental factors and the security of the network in which the device is running.



Device communication in IOT

Section 2: Communication channels(7)

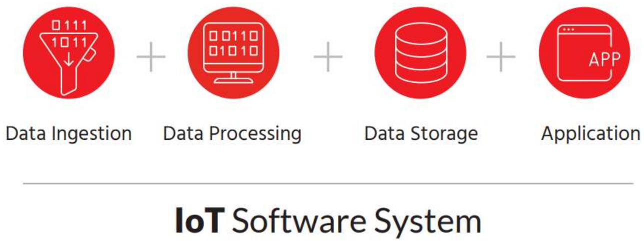
- Quality of Service is a metric to describe the overall performance of a system.
- QoS in IoT systems depends on:
  - Internal communication
  - Communication with the outside world
- Communication is usually resource expensive process in any system.
- QoS can be improved using computation instead of communication whenever possible.



Section 3: Software(1)

- The ability to connect computer-like devices to the internet allows us to utilize remote computing resources. These are not constrained by size, location, power consumption, or network connectivity.
- These computing resources referred to as "**The Cloud**."

- **Components of a cloud:** An IoT deployment, an IoT software system is generally running on Cloud infrastructure, consisting of:
- • Data Ingestion
- • Data Processing
- • Data Storage
- • Application



Section 3: Software(2)

- Tasks of System software

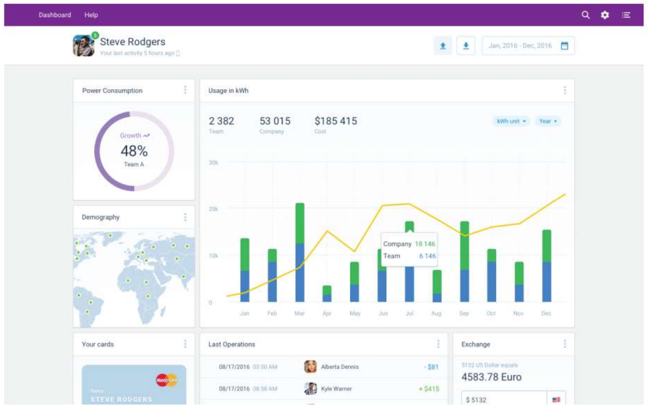
- 1. **Data Ingestion**: The most common task for data ingestion is to listen for and capture the message stream from devices. Technologies include: Apache NiFi, Publish/subscribe model(MQTT), request report model (CoAP)
- 2. **Data Processing**: Its primary function is to apply logic to incoming device data and invoke the corresponding action. Technologies include Lambda and Kappa
- 3. **Data Storage**: NoSQL databases are an obvious choice for storing high volumes of data without having a fixed schema.
- 4. **Application**: An IoT Software Application provides three critical functions:
  - 1. Enables human interaction with the IoT system through a User Interface (UI)
  - 2. Provides a mechanism for data analytics
  - 3. Provides data visualization capabilities

Section 3: Software(3)

- **Using the obtained data**

- **For Data Analytics**:
  - IoT **end-user** can generate analytics using machine learning algorithms to get more insight.
  - Real-time analytics would allow the system to detect deviations from known usage patterns and generate an alert. This can help in managing and detecting anomalies early.

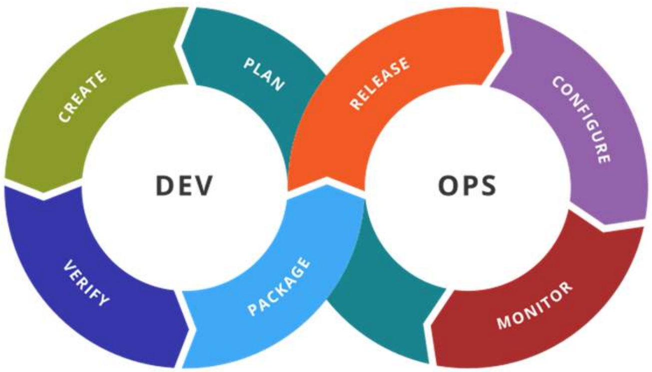
- **For Data Visualization**:
  - Data visualization capabilities provide graphical representations of data, allowing you to spot trends and take appropriate action.
  - You can also embed commercial visualization tools (like Microsoft's PowerBI or Tableau) into an IoT application.



Example **IoT** Dashboard

Section 4: Operations(1)

- An IoT system requires a diversified set of technologies deployed remotely.
- Datacenter infrastructure, the hardware and firmware associated with devices (physical things)



Operation components:

- 1)**Infrastructure**: network, server, and storage infrastructure.
- 2)**DevOps**: Saas concept that development and operations must work together beyond the release of a product or service.
- 3)**Physical things**: firmware updates, battery mgmt., and sensor calibration
- 4)**Security**: protecting the system and everything connected to it.

Section 4: Operations(2)

- **Addressing Security concerns**
  - Edge devices tend to get less attention from systems administrators and, thus, can make an attractive target for hackers.
  - In the rush for convenience, security and privacy are often overlooked. IoT security is still in its infancy, leaving the door open for malicious attacks.
  - IoT devices generally come with very limited processing capabilities. This makes it hard to run state of the art encryption-based security solutions inside the devices.

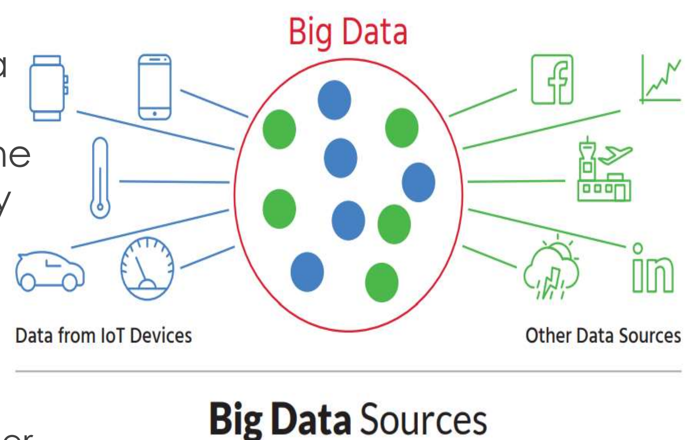
- Using **TLS/SSL encryption**. For this type of communication, private key encryption is stored at the device level.
- **IP white-listing** filters untrusted messages at the device level. This is an easy measure to implement in IoT platforms using a static IP addresses.

IoT devices are vulnerable to common cyber attacks

Section 5: Data

- Big data exists with other small data foundations in the background

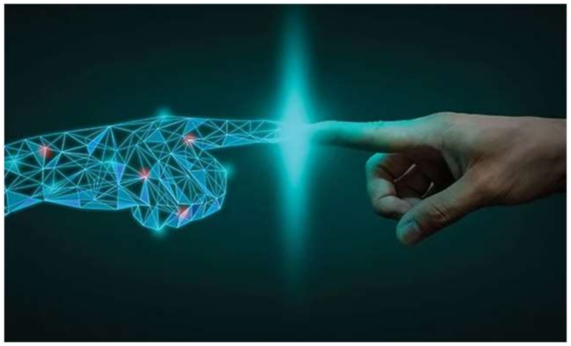
- A critical monitoring system, such as crash detection on a self-driving car, needs to be capable of real-time, local decision-making. The process of sending information to the cloud, processing, and sending commands back is simply too slow, actionable data is needed instantly.



- How small data evolves into big data:
  - Aggregating data from the above example with that of other sources is how small data becomes Big Data.

Concluding thoughts

- While experts may disagree on the projected value of the new Data Economy, they all agree that it will have a greater economic impact than the Internet itself.
- Sensor costs are approaching a level that allows trillions to be deployed annually.
- Big Data analytics and artificial intelligence are at the lowest cost point in history.
- It is easier to develop a connected device now than ever before.



Data and human intelligence

Thank You.