

# Orchestration in the Internet of Things

-

## Towards a fully Integrated Solution

Jonas Burster - 20165136

[jburst16@student.aau.dk](mailto:jburst16@student.aau.dk)

xx.xx.2019

# Contents

---

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Defining Key Terms . . . . .	1
<b>2</b>	<b>Extended State of the Art</b>	<b>4</b>
2.1	Problem Area . . . . .	5
2.2	Candidate Technologies . . . . .	6
2.3	Traditional Gateway Solutions . . . . .	8
2.4	Smart Gateway Solutions . . . . .	8
2.5	Containerized Gateway Solutions . . . . .	10
2.6	Cloud Native Gateway Solutions . . . . .	11

# 1 Introduction

## 1.1 Defining Key Terms

The IoT landscape is often hard to understand, especially as names are defined loosely and inconsistently. The same holds true for the cloud and terms around cluster technology. This section will explain the network topology, key terms and their concepts as the foundation for the following report.

### *Network Topology*

Figure 1 shows the network topology used in this report. The focus will be on the management and security of the device edge as well as its interaction with the IoT devices themselves. The upper layers two layers, the cloud and infrastruc-



Figure 1: Network Topology inspired by [1].

ture edge, and their connections are all operated by big telecompanies and content providers. The cloud is on demand available data storage and processing power. The infrastructure edge is operated by the network providers and is mainly used to provide access to the network to households and companies. It provides some services, e.g. to improve network characteristics such as to lower latency. But, devices operating in this layer are not directly related to IoT and thus excluded in this report.

The device edge is operated by normal households and other non network-related

businesses. It is responsible for the control and data plane of the constrained devices (explained below). The data produced from these devices can be aggregated and processed in this layer. The benefits of doing so are discussed in chapter xxx.

### *Constrained Device*

Constraint devices are the elementary part of the IoT making up the "things" or devices[2]. They can have three main purposes. Either sensing or actuating (or both), where sensing is the passive action of measuring the environment (e.g. a motion detector) and actuating is the active action of influencing the environment (e.g. control of pressure in test tube). Or, finally, they can be smart objects enhancing the interaction between other smart objects and people.

They are usually defined by their limitation, mainly, small computing power (CPU, RAM, storage etc.) and limited power supply and operate in constrained network<sup>1</sup>. In summary, it is fair to assume that many constrained devices have very limited computing power, operate on battery in constrained networks using protocols like BLE and ZigBee.

### *Smart devices*

Smart devices are often not clearly defined in the academic literature, in this report I will use the definition given by Poslad[3], to clearly divide them from constrained devices. They are traditional computing devices and "tend to be multi purpose ICT devices"[3], examples are mobile phones (smart phones) or tablets. They connect to the rest of the infrastructure directly but are free to move between networks. They also often rely on battery power and, importantly, are mainly end user devices. This has important privacy implication when using their computing power for computations on the edge. **(I should pick this up somewhere in**

---

<sup>1</sup>See [2] page 5 for more information.

**the report or go more in detail here).**

### ***IoT Gateway***

IoT Gateways are the connection between smart devices and a network, this could be a local network or even the Internet. They facilitate inter-network and intra-network communications and because smart devices and especially constrained devices often communicate via wireless and non-Internet protocols, IoT gateways often translate protocols "between wireless sensor networks [...] traditional communication networks"[4]. In recent years IoT Gateways have become a major field of interest and new research. As these devices got more powerful, developers started using them for preprocessing and datagathering locally at the edge. In conclusion, IoT gateways can take a wide variety of forms. They can be simple L3 routers or more powerful devices. Importantly, they are situated at the edge of a network and act as bridge between two autonomous systems.

### ***Edge node***

Edge nodes are defined as nodes "that act as an end user portal for communication with other nodes in cluster computing"[5]. It operates on the edge, it must be able to run containers, has far inferior processing power compared to servers and can (only) run as a worker node (also known as a minion in kubernetes)[6]. Note that, this is in contrast to IBM which defines edge nodes as ingress traffic nodes in a cluster[7]. In this report an edge node is a powerful IoT gateway situated at the edge of the network. Because of new and exciting developments it will not be restricted by the type of software it can run (it can thus be a master node as well), but rather by its network topology and mobility. It is a node without reliable and fast connection to the rest of the network, does not need a static IP

and is (somewhat) portable<sup>2</sup>. Reoccurring themes are the restrictions compared to cloud clusters, which are smaller processing power, no permanent connection to the backbone network and greater portability.

### ***Edge cluster***

The term edge cluster is closely related to cluster technologies like Kubernetes or Mesos. Edge clusters are computers powerful enough to run a full control plane of the cluster technology. However, there is no clear definition of what constitutes to an edge cluster in neither the academic literature nor the industry. They are more powerful edge nodes, often packing additional hardware like GPUs or SSDs. However, emerging technologies like tiny builds of a full Kubernetes cluster like K3s from Rancher Labs[8] make this distinction between edge nodes and edge clusters increasingly difficult <sup>3</sup>.

Because of their similarities, in this report the distinction between edge nodes and clusters will be solely made up on the cluster topology separating them on an architectural level.

## **2 Extended State of the Art**

What is the purpose of this section?

problem area: what is actually the problem with the current system? hint into solution

competitor analysis: compare different approaches to solve the management and security of IoT gateways as well as solutions inside the individual categories.

---

<sup>2</sup>Comparing edge nodes to cloud nodes is also common academic practice[2] but not considered at this point.

<sup>3</sup>Rancher provides a 40MB Kubernetes binary and claims that 500MB of RAM is sufficient it stable.

## 2.1 Problem Area

IoT has seen a rapid growth over the last few years. According to IoT Analytics the total number of IoT devices is set to surpass the total number of other connected devices around 2021 [9]. Further, most IoT devices will be used in WPAN<sup>4</sup> and WLAN<sup>5</sup>. Traditionally these devices connect to the enterprise or service provider core networks through a gateway. This gateway was mainly a router operating at L3<sup>6</sup> to route packets and translate between different types of network protocols. [10]. However, according to Dejan Bosanac, a senior software engineer at Red Hat in the field of cloud messaging and IoT platforms, due to their proximity to the sensors and the end user, these devices have three main advantages over the cloud: "Low latency, availability and locality" [11]. Because of this advantage system designers started to construct hybrid systems, in which the gateway plays an active role in the data processing pipeline. This architectural style of carrying out substantial amount of computation and storage at the edge is called "fog computing" [12] and a simple example can be seen in figure 2.



Figure 2: IoT Device Setup [1].

But fog computing does not come without its drawbacks. Depending on the protocol edge devices need to be close to their peers and slaves and physically

<sup>4</sup>Wireless Private Area Networks includes technologies like Zigbee, Z-wave and Bluetooth

<sup>5</sup>Wireless Local Area Networks includes mainly Wi-Fi

<sup>6</sup>L3 stands for Layer 3, the networking layer in the OSI model.

accessible for maintenance. Which also poses a major security risk as they could be accessed by malicious intruders. The software maintenance is another critical aspects. Often IoT and edge devices are not update and patched with critical consequences. The "2016 Dyn cyberattack" used IoT devices like residential gateways, smart fridges, baby phones ect. to bring down the DNS-Servers operated by Dyn making large part of the Internet inaccessible for hours[13]. The authors also stress that "large number of IoT devices are accessible over public Internet" and that "security (if considered at all) is often an afterthought in the architecture of many wide spread IoT devices"[13].

The question is then, how can manage and secure those devices. In this report, I will solely be concerned with the software aspect, which can mitigate some effects of exposing physical hardware to more accessible places.

Many challenges facing edge devices today have already been solved, although in a slight different context: The cloud[11]. In the cloud

## 2.2 Candidate Technologies

Traditionally, edge devices were isolated gateways mainly forwarding traffic from their slaves to the cloud. This meant, all processing and storing was done in the cloud. Thus, the software of the gateways didn't need much management or maintenance. With advent of increased processing and storage at the edge, so called fog computing, the software on the gateways expanded to include business logic as well as routing. Today, gateways can be an integral part of the data flow, pre-processing data, filtering and storing data. However, this new software needs much more maintenance and management because changes in the business logic, e.g. API changes, need to be implemented in the gateway as well as on all other connected devices. With the advent of IIoT, the number of IoT gateways is set to increase dramatically and thus a solution for this problem has to be found.