Edge Computing Security

Javier Lopez

Network, Information and Computer Security (NICS) Lab

University of Malaga

(joint work with Rodrigo Roman, Ruben Rios and Jose A. Onieva)

FOSAD 2019

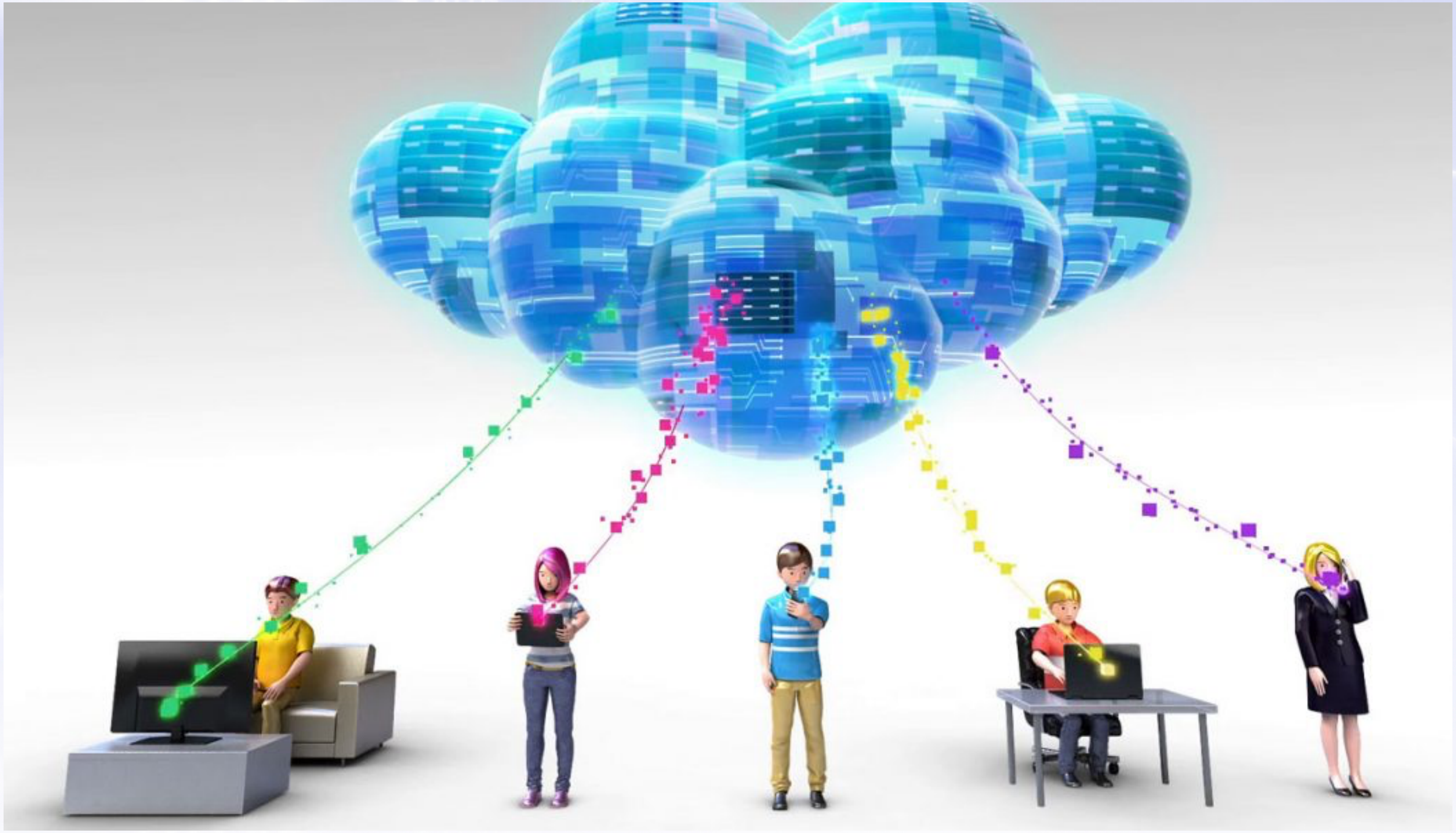
Outline

- **DAY 1**
  - Edge Computing Paradigm(s)
  - The Ecosystem
  - Security Threats and Mechanisms

- **DAY 2**
  - Main Edge Architectures: OpenFog and MEC
  - Security in OpenFog and MEC
  - Research on Edge Security Mechanisms
  - Edge Computing as a Security Enabler
  - Examples of Using the Edge for Enhanced Security

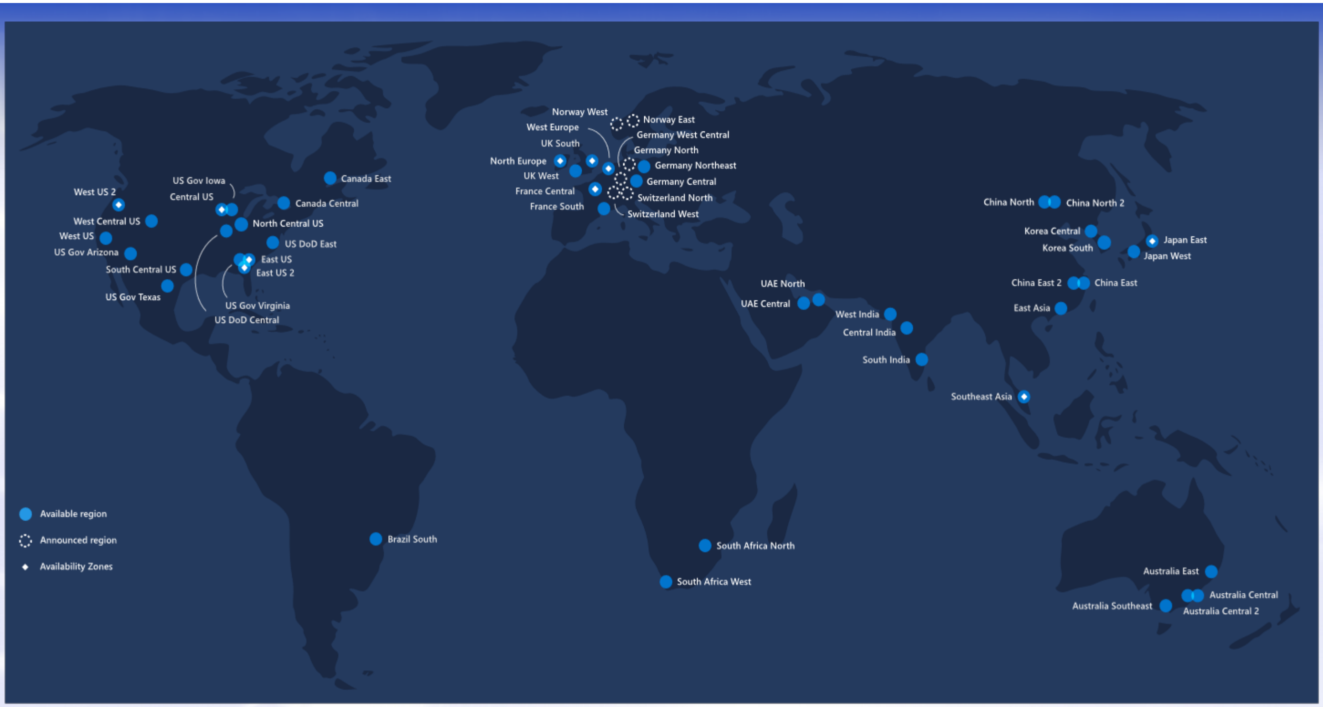
EDGE COMPUTING PARADIGM(S)

Cloud Computing

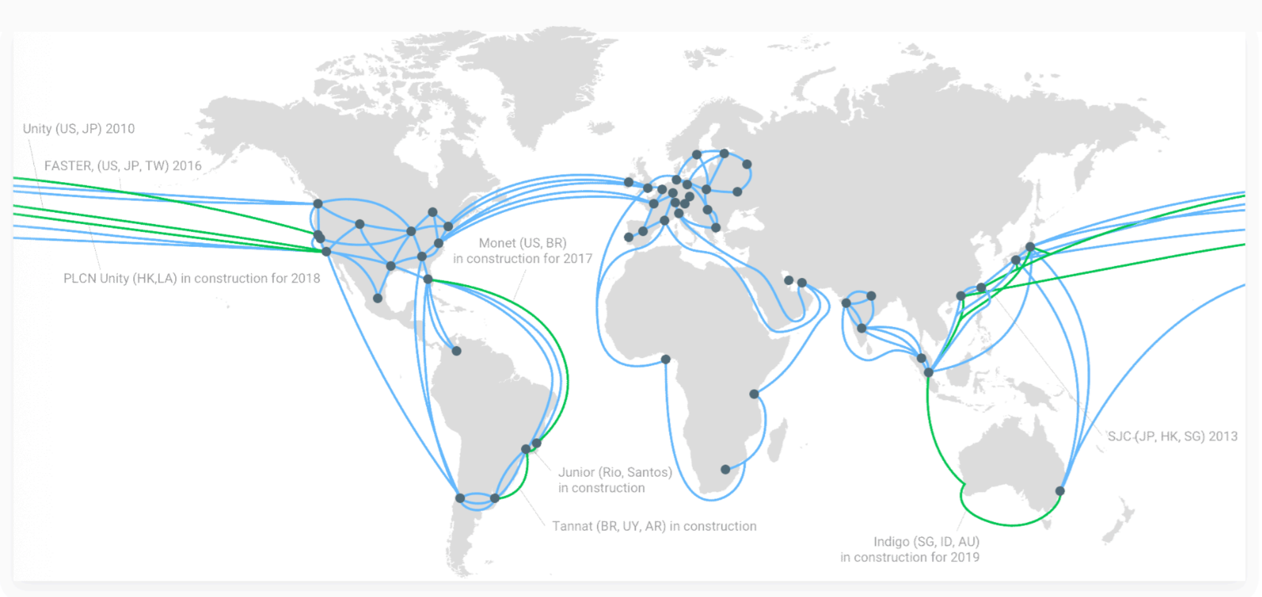


Cloud Computing

Cloud Computing



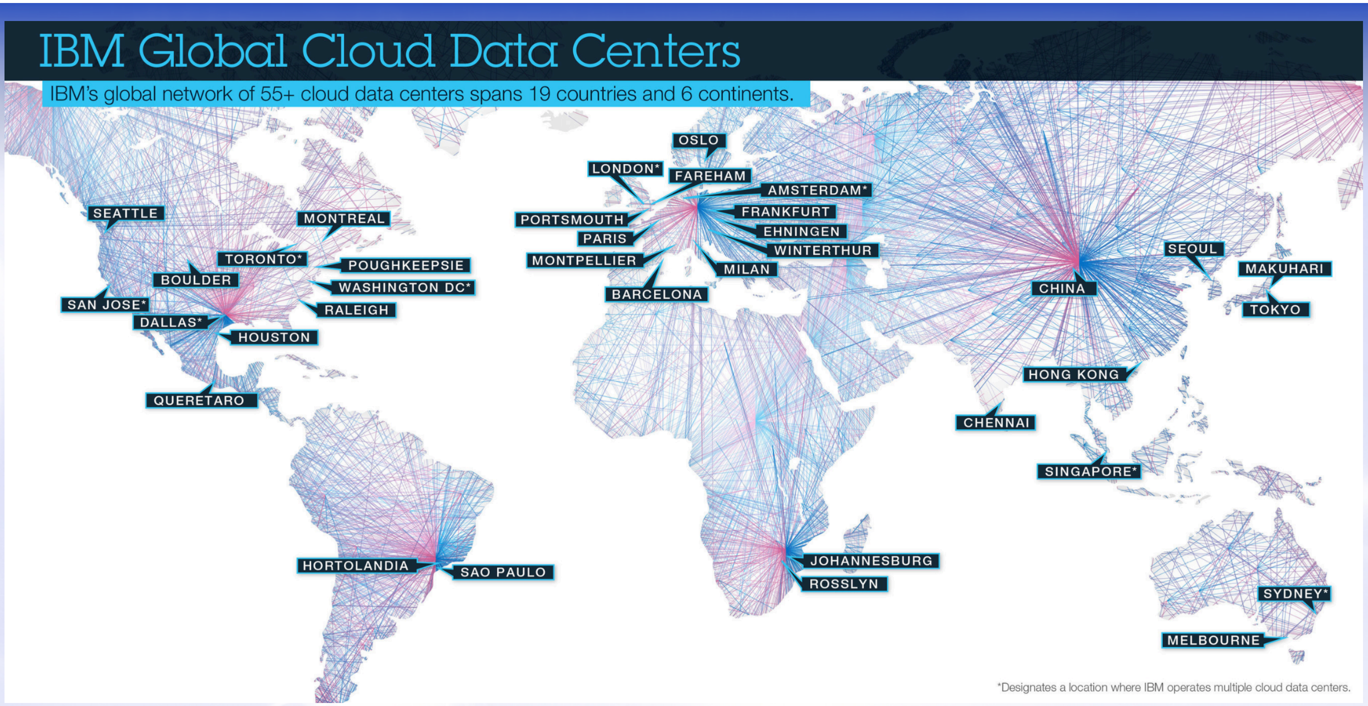
AWS Global Infrastructure Map



— Google Cloud Platform network

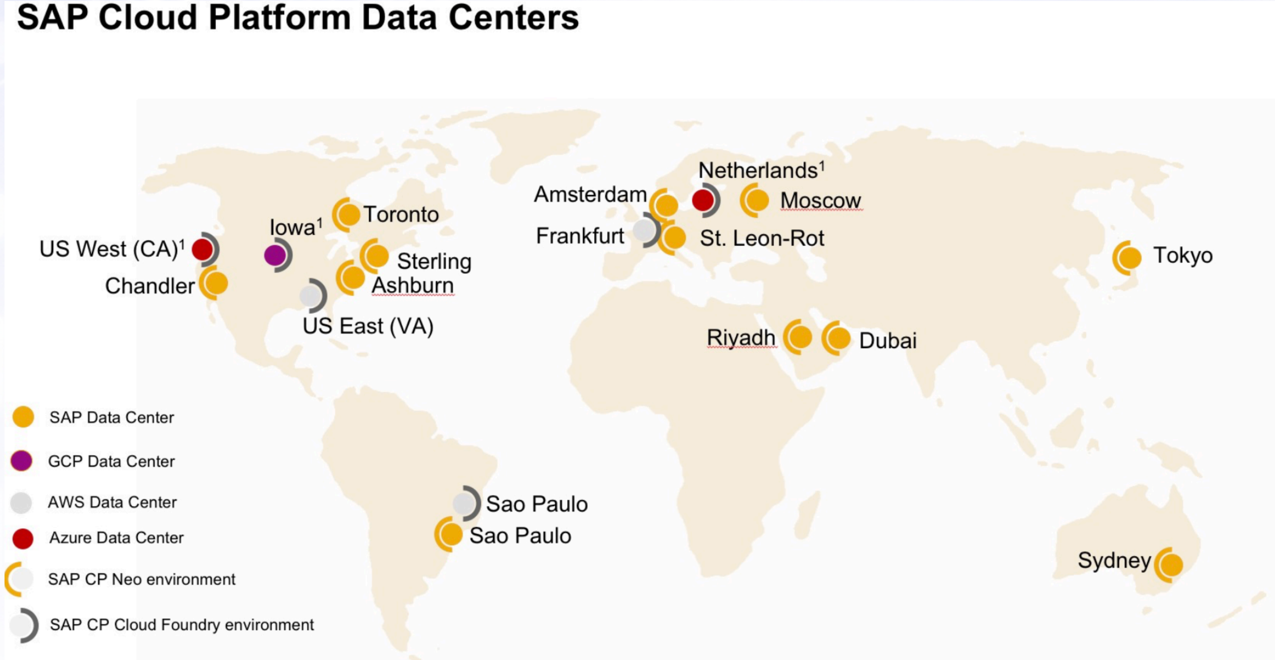
IBM Global Cloud Data Centers

IBM's global network of 55+ cloud data centers spans 19 countries and 6 continents.

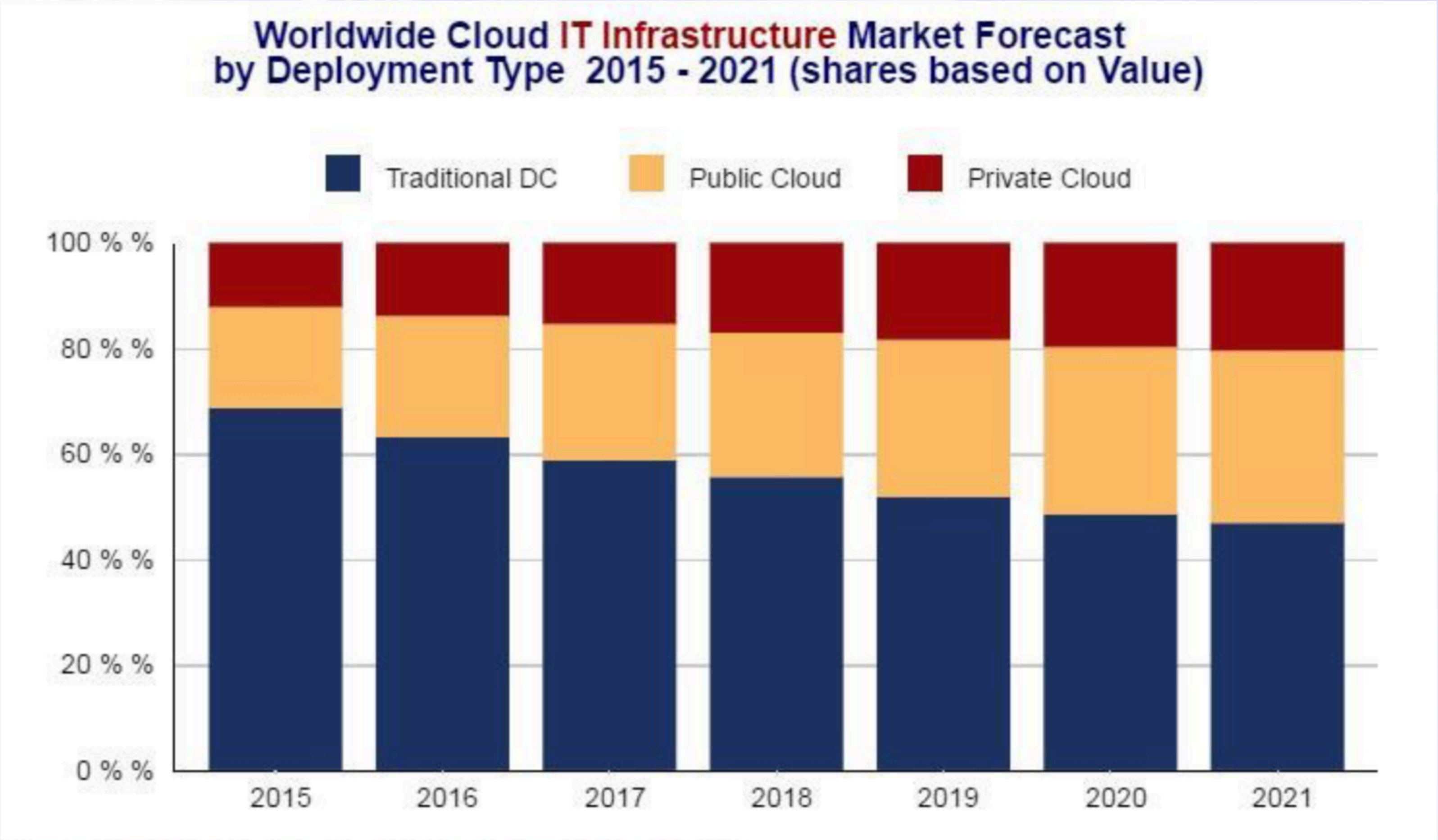


*Designates a location where IBM operates multiple cloud data centers.

SAP Cloud Platform Data Centers

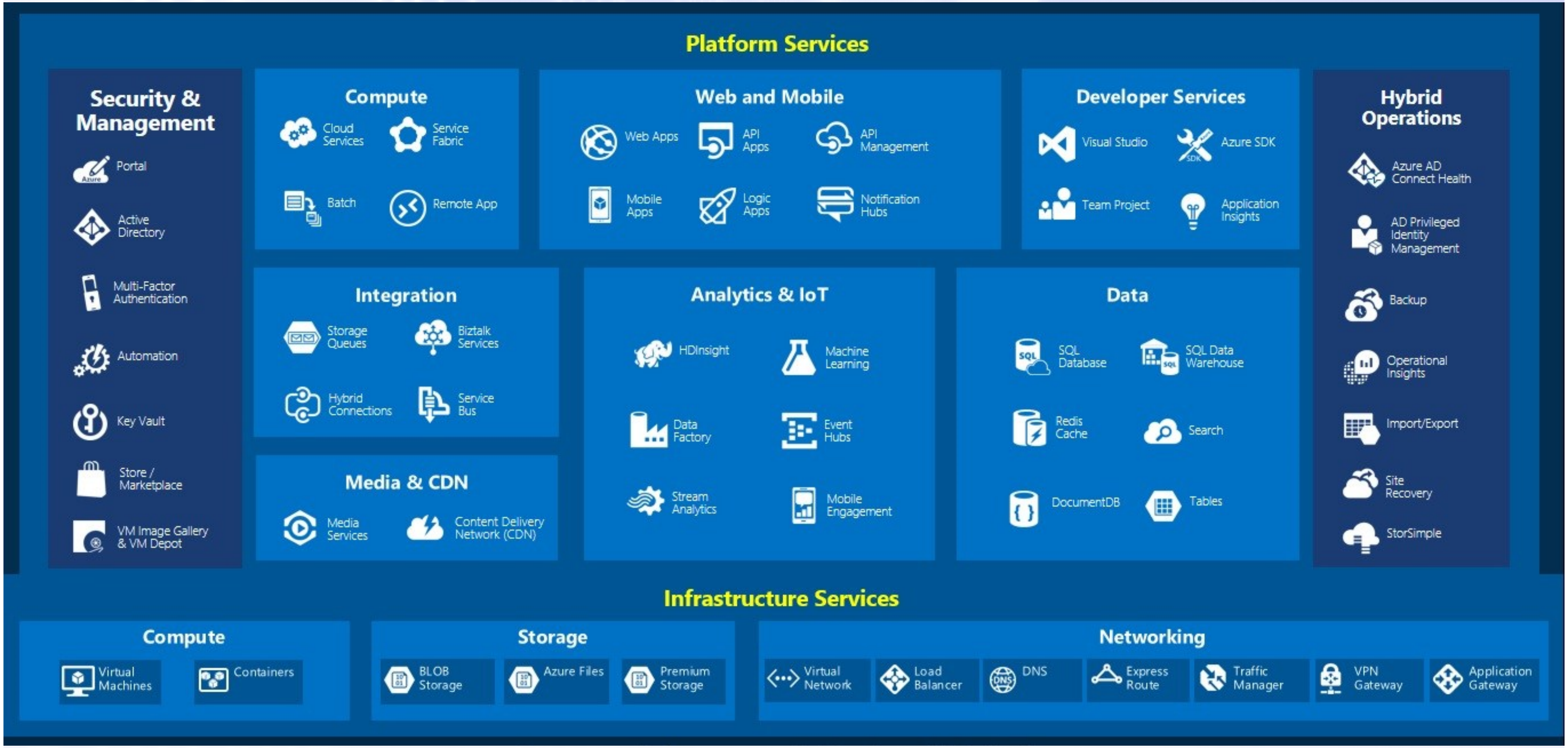


Cloud Computing



IDC Analyze the Future

Cloud Computing



Platform Services

Security & Management

- Portal
- Active Directory
- Multi-Factor Authentication
- Automation
- Key Vault
- Store / Marketplace
- VM Image Gallery & VM Depot

Compute

- Cloud Services
- Service Fabric
- Batch
- Remote App

Web and Mobile

- Web Apps
- API Apps
- API Management
- Mobile Apps
- Logic Apps
- Notification Hubs

Developer Services

- Visual Studio
- Azure SDK
- Team Project
- Application Insights

Hybrid Operations

- Azure AD Connect Health
- AD Privileged Identity Management
- Backup
- Operational Insights
- Import/Export
- Site Recovery
- StorSimple

Integration

- Storage Queues
- Biztalk Services
- Hybrid Connections
- Service Bus

Media & CDN

- Media Services
- Content Delivery Network (CDN)

Analytics & IoT

- HDInsight
- Machine Learning
- Data Factory
- Event Hubs
- Stream Analytics
- Mobile Engagement

Data

- SQL Database
- SQL Data Warehouse
- Redis Cache
- Search
- DocumentDB
- Tables

Infrastructure Services

Compute

- Virtual Machines
- Containers

Storage

- BLOB Storage
- Azure Files
- Premium Storage

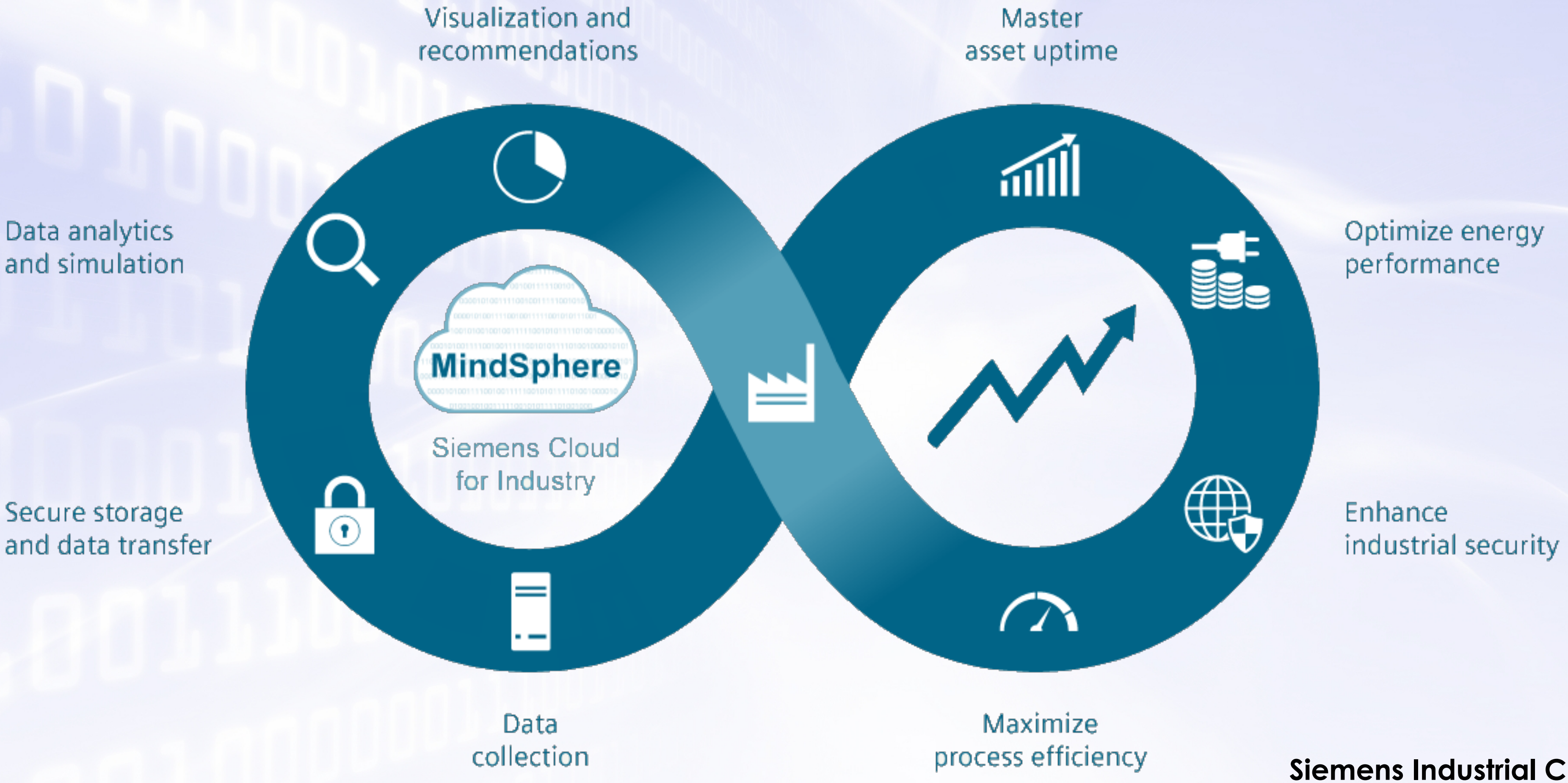
Networking

- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- Application Gateway

Microsoft Azure - https://azure.microsoft.com

From IT Infrastructures…

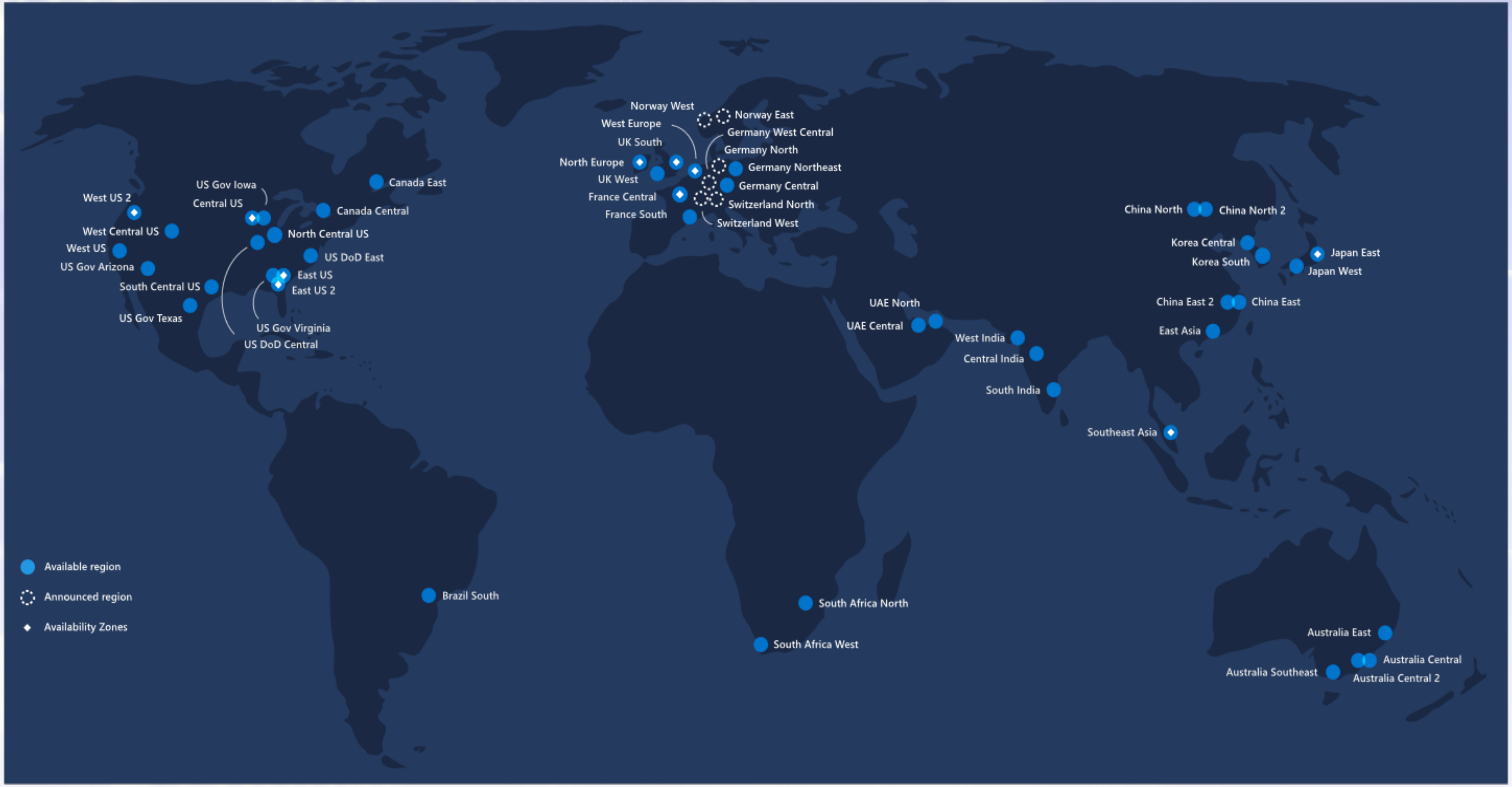
Cloud Computing


Visualization and recommendations
Master asset uptime
Data analytics and simulation
Optimize energy performance
MindSphere
Siemens Cloud for Industry
Secure storage and data transfer
Enhance industrial security
Data collection
Maximize process efficiency

Siemens Industrial Cloud

...to high-level applications/services backed by the cloud

Cloud Computing: The Panacea?



AWS Global Infrastructure Map

- ➢ Any issues if we delegate the execution of our processes to an infrastructure that is "far away" ?

- *Once upon a time …*

- Researchers in the area of mobile computing start worrying… about the inherent resource poverty of mobile devices … in the particular case of resource-intensive mobile services

> *"While mobile elements will undoubtedly improve in absolute ability, they will always be at a relative disadvantage"*
>
> M. Satyanarayanan, Carnegie Mellon Univ.

- Start exploring different options:
  - strictly local execution
  - strictly remote execution:
    - information of the mobile client is sent to a remote server for processing, and the result is sent back to the client
  - hybrid execution:
    - some preliminary processing done locally, and specific extracted information is sent to a remote server for completing the process

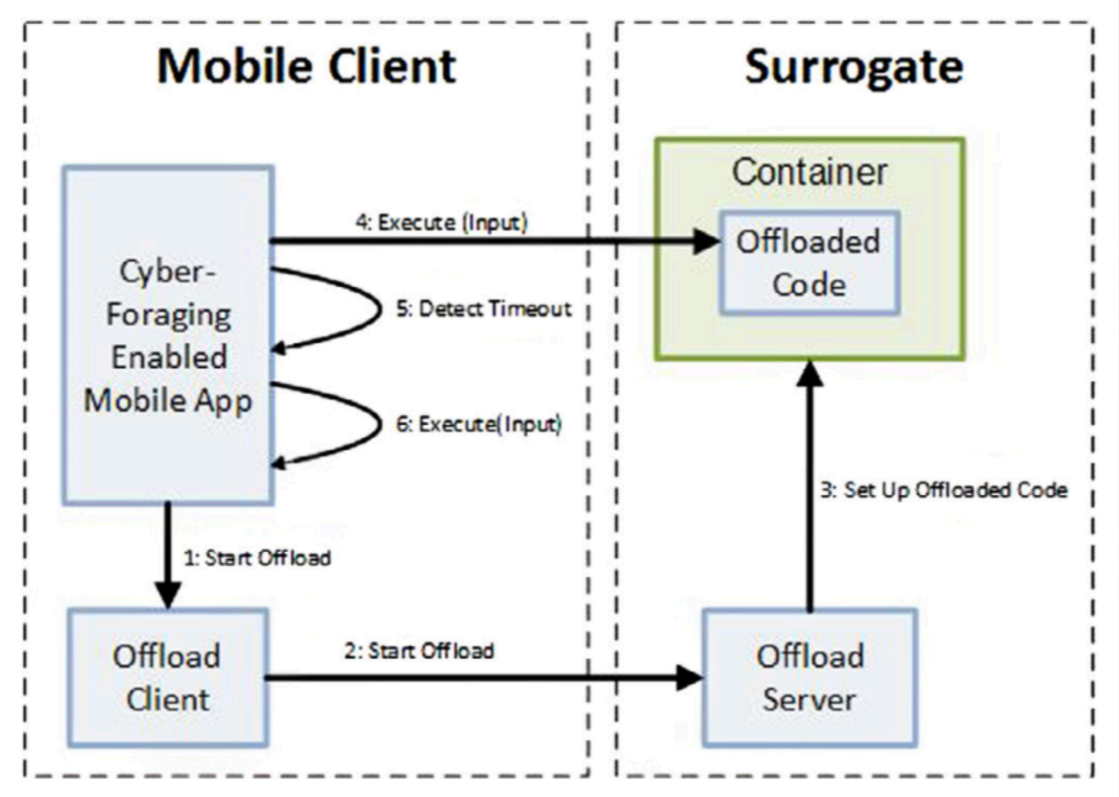
- Preliminary experiments show them that leveraging "nearby" resources is the best approach for resource poverty problem
  - mainly because of energy/battery saving

Cyber Foraging

- A new term is coined, *cyber foraging*:
  - dynamically increase the computing resources of a wireless mobile device by exploiting wired HW infrastructure
  - resource-poor mobile devices offload some of their heavy work to stronger surrogate "nearby" computer(s)

- Considered a must: Low latency and high bandwidth to the remote execution site

- Problem:
  - the term "nearby" is not precisely specified



Cyber Foraging

- Important issues to answer:
  - Where will remote execution be performed?
  - Who will provide that infrastructure for cyber foraging?
  - How will trustworthy computers for remote execution be dispersed in the environment?
  - How will mobile devices discover them?
  - What business incentives will there be in order to deploy and maintain such infrastructure?

Mobile computing meets Cloud computing

- In parallel, and independently of mobile computing considerations:
  - A few big companies start making computing resources available on the Internet that can be used for transient purposes
  - Let’s call it Cloud Computing
- Hence, the emergence of Cloud Computing brings (by chance?) the business model and the incentive:
  - for deploying and maintaining computers for remote execution
- Therefore, all problems related to remote execution of mobile computing are finally solved!!
  - really? …

Mobile computing meets Cloud computing

- FACT: The economics of cloud computing strongly favor the centralization of infrastructure into a few large data centers.

- More in detail, it is through economies of scale in:

  (i) operations, and

  (ii) system administration

  that cloud computing wins.

West US 2
US Gov Iowa
Central US
Canada East
Canada Central
West Central US
North Central US
West US
US Gov Arizona
US DoD East
East US
East US 2
South Central US
US Gov Texas
US Gov Virginia
US DoD Central
Norway West
Norway East
West Europe
Germany West Central
UK South
Germany North
North Europe
Germany Northeast
UK West
Germany Central
France Central
Switzerland North
France South
Switzerland West
China North
China North 2
Korea Central
Korea South
Japan East
Japan West
UAE North
UAE Central
China East 2
China East
East Asia
West India
Central India
South India
Southeast Asia
Available region
Announced region
Availability Zones
Brazil South
South Africa North
South Africa West
Australia East
Australia Central
Australia Southeast
Australia Central 2

AWS Global Infrastructure Map

Mobile computing meets Cloud computing

- Therefore, researchers on mobile computing area claim that cloud computing is not the panacea because:
  - it tends to occur that there is a large average separation between a mobile device and its cloud
  - therefore, end-to-end communication involves many network hops, and results in high latencies

- And, further, they claim that this is particularly problematic in latency-sensitive and compute-intensive applications
  - such as face recognition, object recognition, and augmented reality.

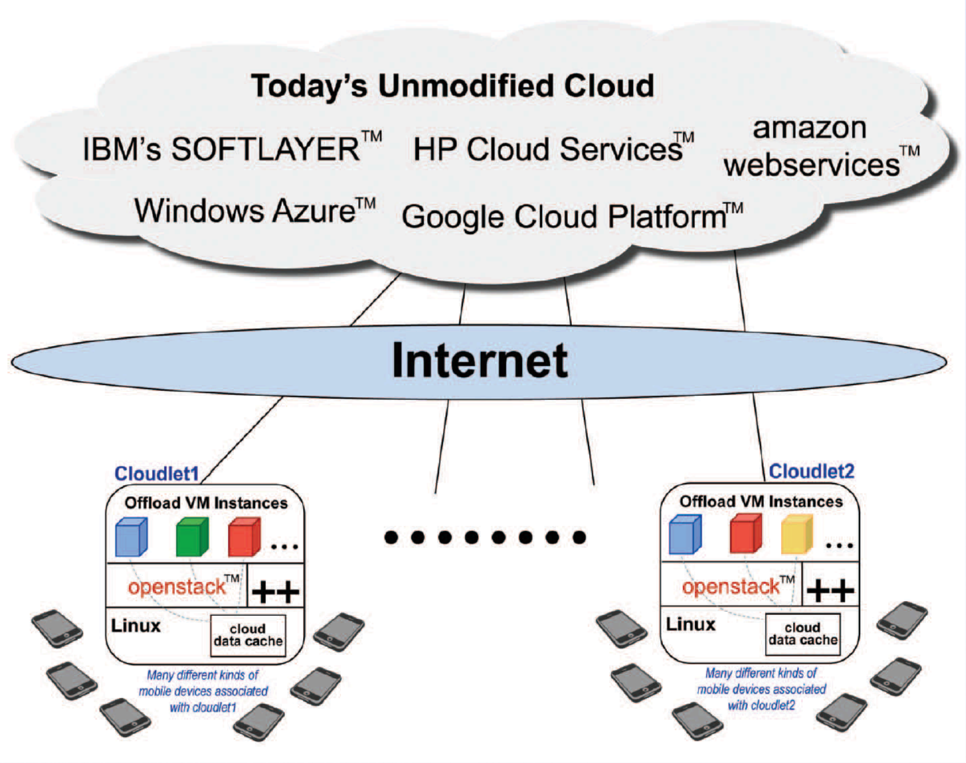
- In conclusion, proximity matters!!

Mobile-Cloud convergence: Cloudlets

- For this reason, it is proposed a two-tier architecture for mobile-cloud convergence

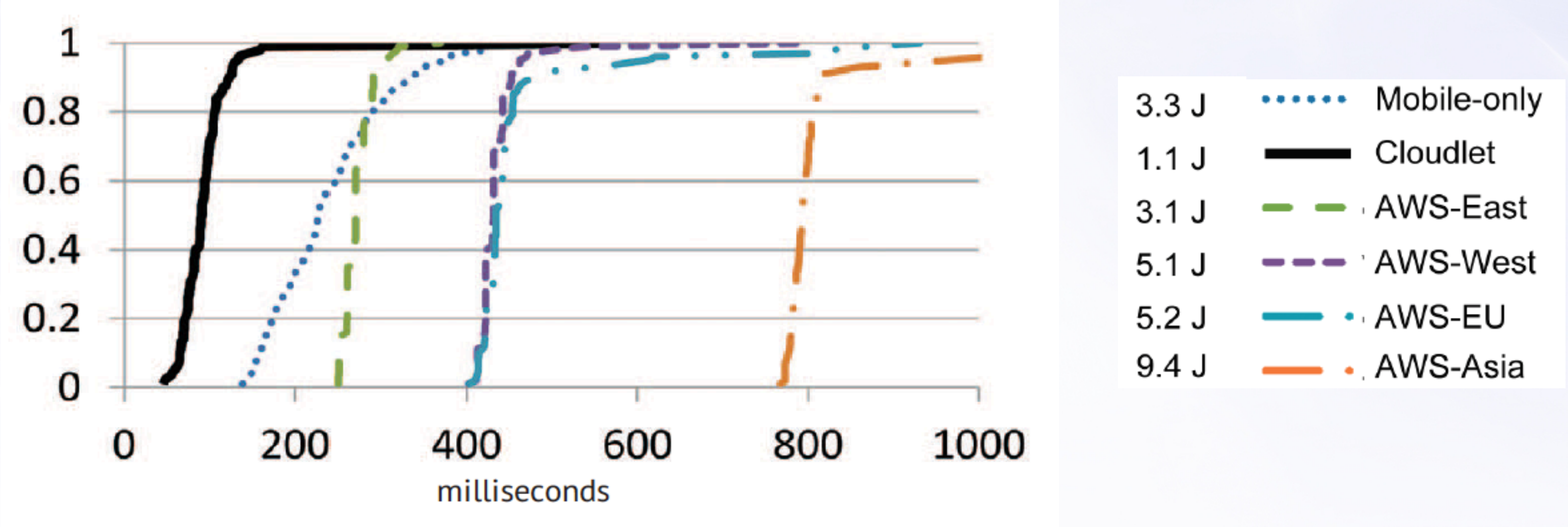
- First level is the cloud infrastructure, while second one consists of dispersed elements called *cloudlets*
  - A cloudlet is a one-hop-away second-class data center

- Is this architecture really necessary?



Cloudlets and Mobile Cloud Computing

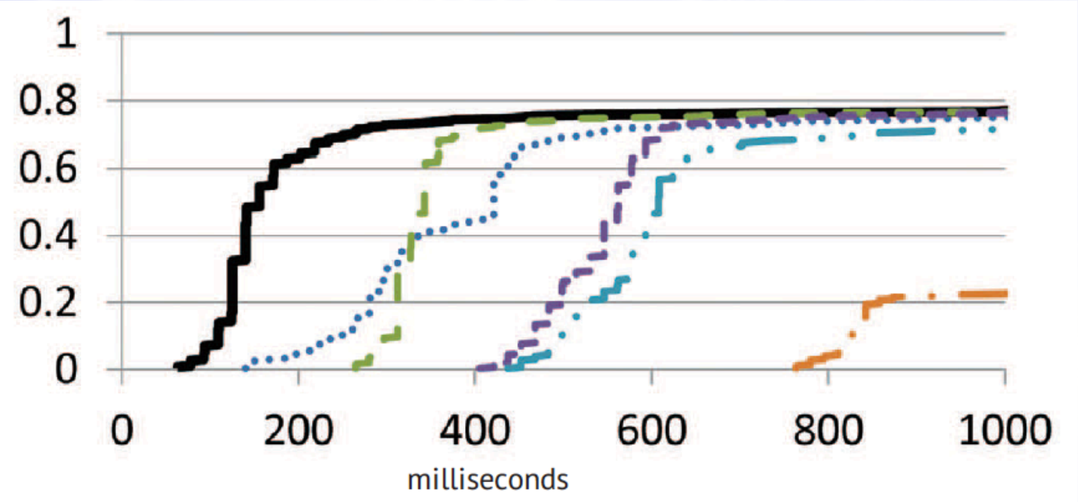
- Some tests performed at Carnegie-Mellon
  - An image from the mobile device is sent over a Wi-Fi first hop to different Amazon Web Services (AWS) data centers
    - … and to a cloudlet
  - The image is processed at the destination
  - For the augmented reality app, buildings in the image are recognized, and labels of their identities are transmitted back to the mobile device



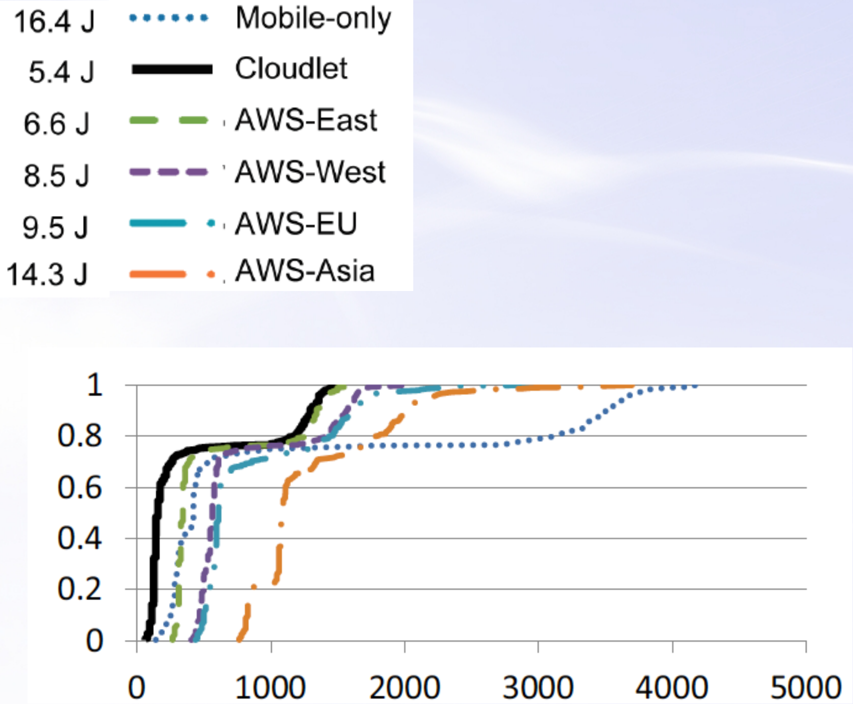
(a) Augmented Reality

Cloudlets and Mobile Cloud Computing

- For the face recognition application, the identity of the person is returned after processing the image at destination.



(b) Face Recognition



- Conclusions of the tests performed:
  - End-to-end latency plays a dominant role.
  - Increasing response time also increases the energy consumption on the mobile device.
  - Similar results (as AWS) with any offload service that is concentrated in a few large data centers.

Cloudlets and Mobile Cloud Computing

- In summary:
  - Cyber foraging lies at the intersection of mobile and cloud computing, giving rise to the **Mobile Cloud Computing** paradigm
  - It dynamically augments the computing resources of mobile devices by exploiting fixed computing infrastructure in the surrounding
    - Surrogates are geographically distributed to be as close as possible to mobile computers
  - Applications functionality is dynamically partitioned between the mobile device and infrastructure servers, that store data and execute computation
  - The location of application functionality changes in response to: (i) user mobility, (ii) platform characteristics, and (iii) variation in resources such as network bandwidth and CPU load
  - Therefore, clusters of mobile devices may provide the same functionality

Fog Computing

- IoT features like:
  - ultra-largescale network of things
  - device and network level heterogeneity
  - large numbers of events generated

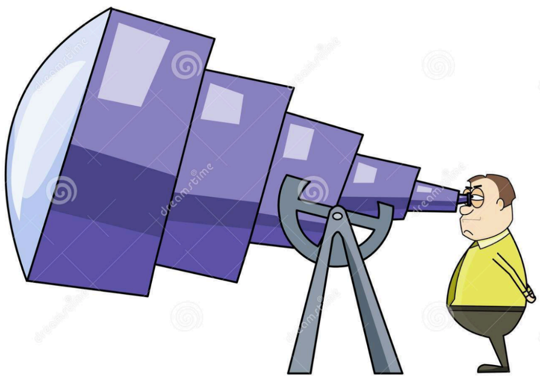
  facilitate development of emerging applications and services.

- The great amount of heterogeneous data collected by IoT needs to be stored and processed
  - and the obtained insights retrieved for visualization or actuation.

- But all these tasks can rarely be performed on the objects themselves
  - as they typically have limited compute, storage, and networking resources, and can be battery-powered.

- Therefore, the IoT needs support from more powerful resources, like Cloud Computing resources.

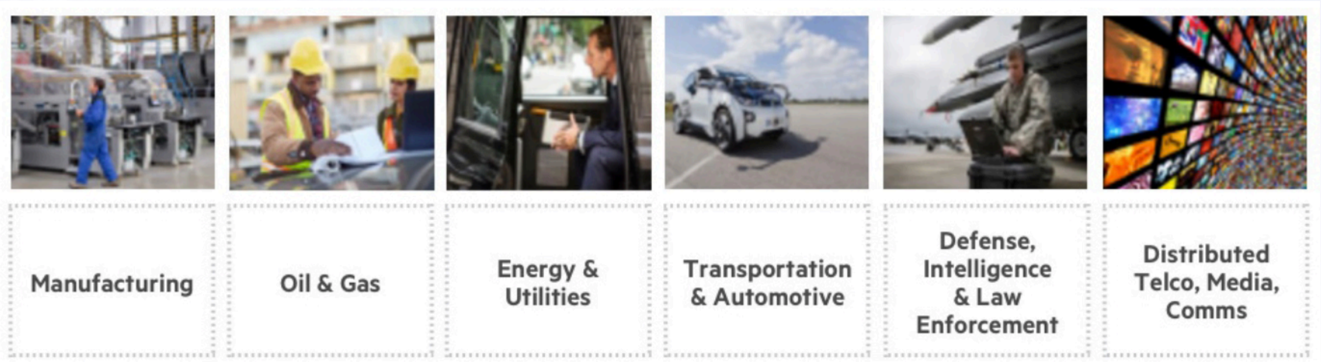
Fog Computing



- However, cloud resources are far away from most of data producers and consumers.

- Besides, and as thoroughly claimed by CISCO:
  - IoT features introduce new challenges that cannot be adequately addressed by the centralized cloud computing architecture.

- CISCO argues that this is specially true in sectors such as manufacturing, oil and gas, utilities, transportation, …
  - where faster response time can improve output, boost service levels, and increase safety.

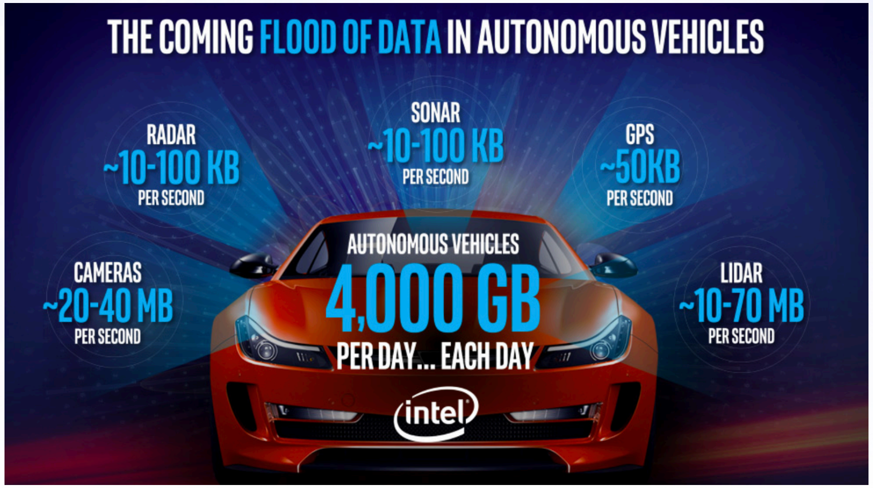

Manufacturing
Oil & Gas
Energy & Utilities
Transportation & Automotive
Defense, Intelligence & Law Enforcement
Distributed Telco, Media, Comms

Fog Computing

- Latency
  - A number of IoT application domains fall under the Ultra-Reliable Low-Latency Communications (URLLC) category
  - This means that extremely low and predictable response times are of utmost importance
  - For instance:
    - Road safety and autonomous driving services require latencies of less than 50ms
    - Smart Grids require latencies up to 20ms
    - Smart Factories have the most stringent requirements, with latencies varying from 250μs to 10ms.

Fog Computing

- Bandwidth consumption
  - The number of objects producing and/or consuming data is projected to exponentially increase within the next few years
  - ABI Research estimates that data captured by IoT devices is expected to exceed 1.6 zettabytes (i.e., 1600 billion gigabytes) by 2020
  - For example:
    - a smart factory might produce over 1000 terabytes a day
    - self-driving cars may generate one gigabyte a second
    - smart meters (only in US) collect energy consumption data at 53.6 petabytes a year



Fog Computing

- Context-awareness
  - Context awareness enables provision of improved services and resources utilization
  - Examples of context information:
    - the set of nearby nodes and/or services
    - local network conditions and traffic statistics
  - However, limited context is shared between a cloud data center and the sensor/actuator nodes
    - disaggregation between them mainly due to lack of proximity
  - For instance:
    - if a cloud-hosted service detects a car accident at a road intersection, it would not be able to inform other vehicles in the vicinity of the accident, due to lack of local context.

Fog Computing

- Privacy and Security
  - The use of IoT objects leads to the collection of sensitive data (e.g.: health-related data) that needs adequate protection
    - Transmitting these data over the public Internet to a Cloud data center may incur privacy risk
  - Besides, IoT objects may not have enough resources to encrypt/decrypt data, hence C-I-A triad is at risk.
  - Legal implications may raise when sensitive data collected in one country are transmitted to a cloud data center in another country with different regulations
    - an aspect that has become more significant with the recent GDPR legislation in Europe

Fog Computing

- In order to overcome those *limitations of integration between IoT and cloud data centers*, CISCO proposes **Fog Computing** paradigm

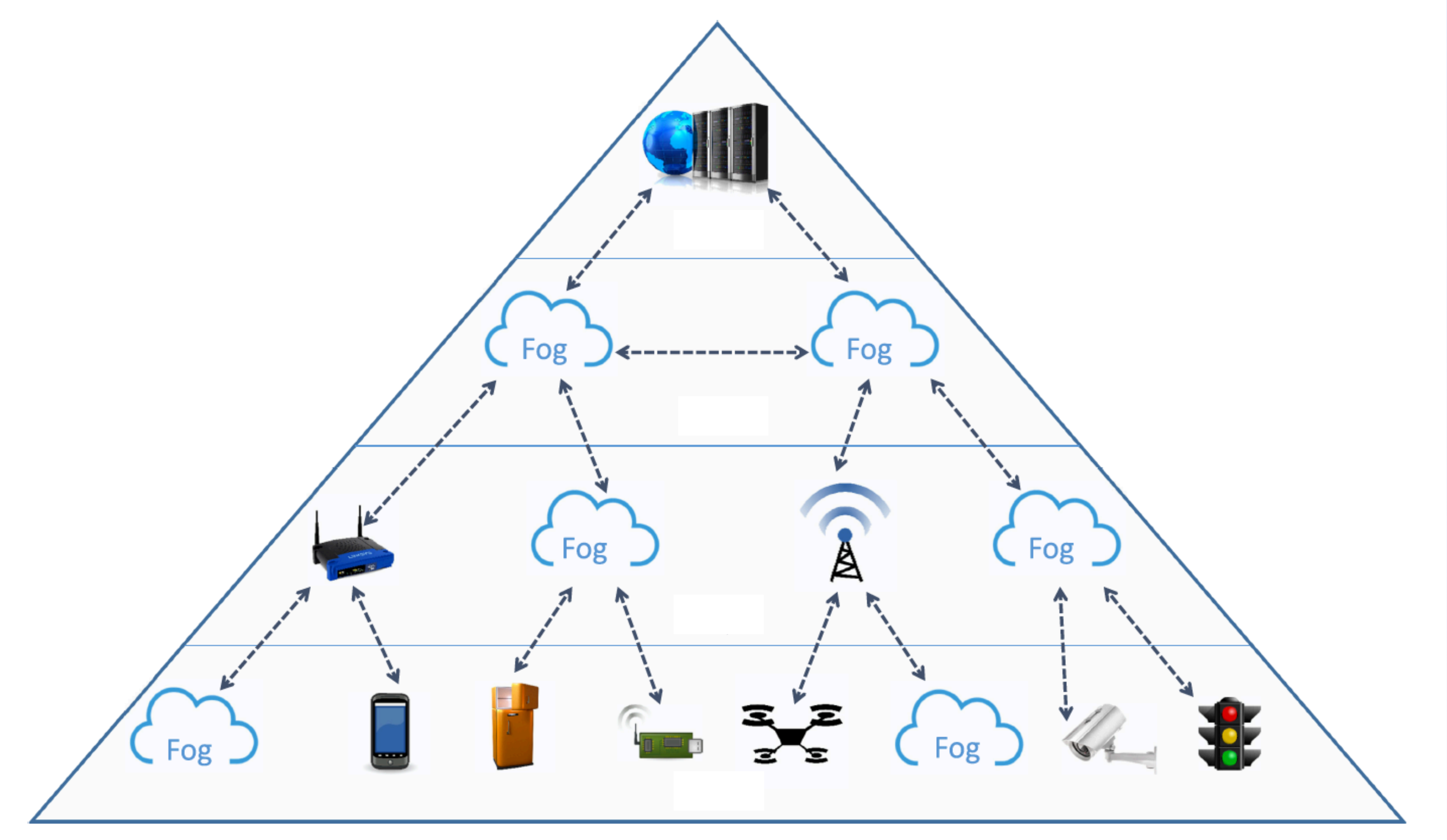
"Fog computing is a horizontal, system-level architecture that distributes computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum."

- Fog services may be distributed anywhere along the continuum from cloud to objects, hosted on nodes known as Fog Nodes.

- A Fog Node can be any device that has enough computing, storage, and networking capabilities to run advanced services:
  i. specialized core network routers;
  ii. advanced switches, gateways, **Wi-Fi access points**, cellular base stations;
  iii. resource-rich end devices (e.g.: vehicles, traffic lights, indust. controllers, …)

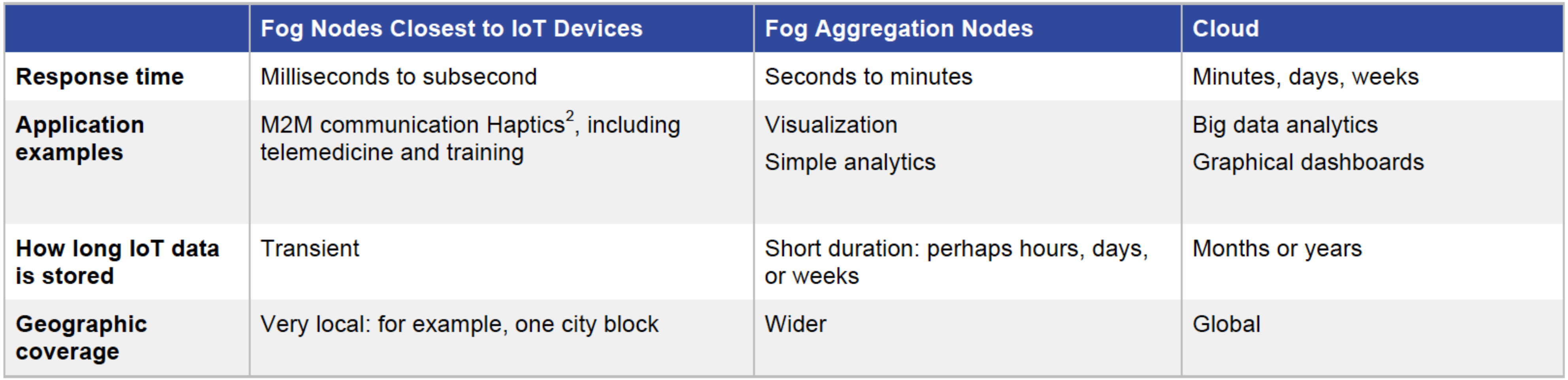
Fog Computing

- Fog computing is not conceived to replace the Cloud but to coexist and cooperate
  - many services require the characteristics of both the Fog and the Cloud.



Fog Computing

- In summary, according to CISCO, fog computing must be considered when:
  - Data is collected at the extreme edge: vehicles, ships, factory floors, roadways, railways, etc.
  - Thousands or millions of things across a large geographic area are generating data.
  - It is necessary to analyze and act on the data in less than a second.



	Fog Nodes Closest to IoT Devices	Fog Aggregation Nodes	Cloud
Response time	Milliseconds to subsecond	Seconds to minutes	Minutes, days, weeks
Application examples	M2M communication Haptics^2, including telemedicine and training	Visualization Simple analytics	Big data analytics Graphical dashboards
How long IoT data is stored	Transient	Short duration: perhaps hours, days, or weeks	Months or years
Geographic coverage	Very local: for example, one city block	Wider	Global

Multi-Access Edge Computing (MEC)

- IBM and Nokia introduced the first computing platform that could run applications/services directly within a mobile base station
  - that is, at the edge of the telecom network

- From there, ETSI has moved towards:

  (i) evolution of mobile base stations, and

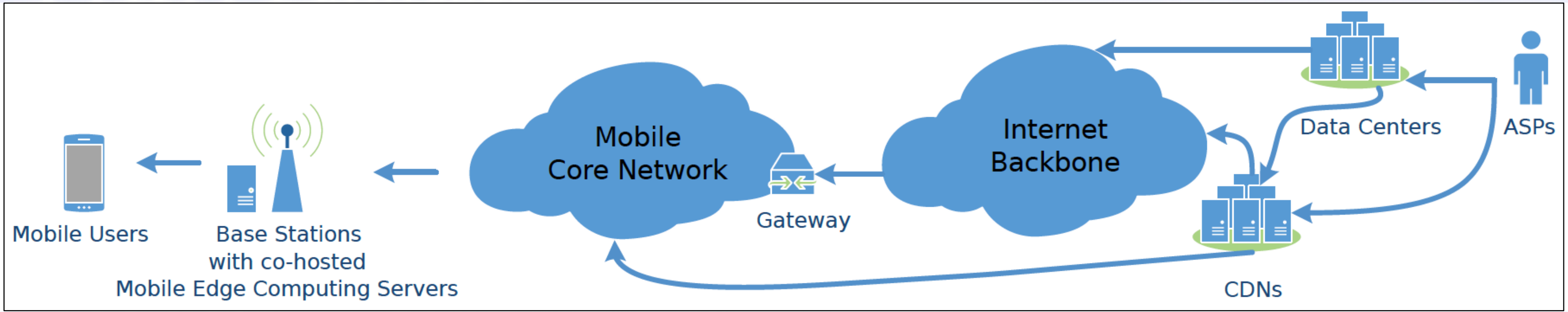
  (ii) convergence of IT and telecommunications networking.

- More precisely, ETSI aim has been to provide an IT service environment + cloud computing capabilities in those stations
  - hence creating the concept of **Mobile Edge Computing (MEC)** paradigm
  - later renamed as **Multi-Access Edge Computing**

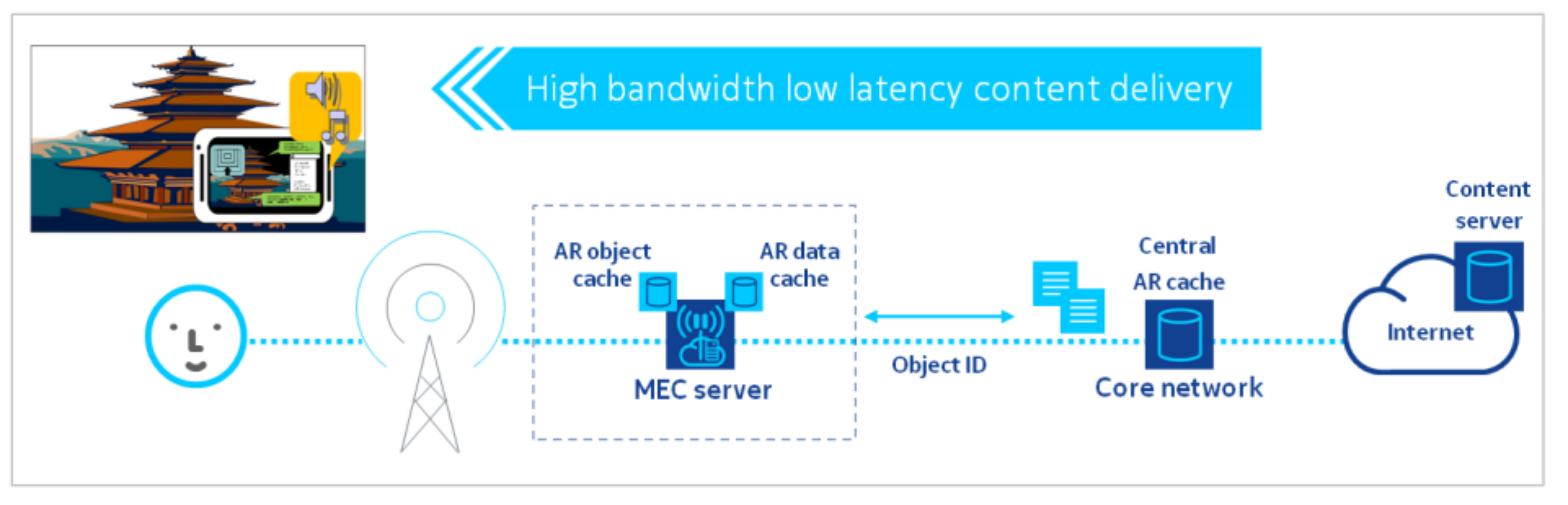
Multi-Access Edge Computing (MEC)

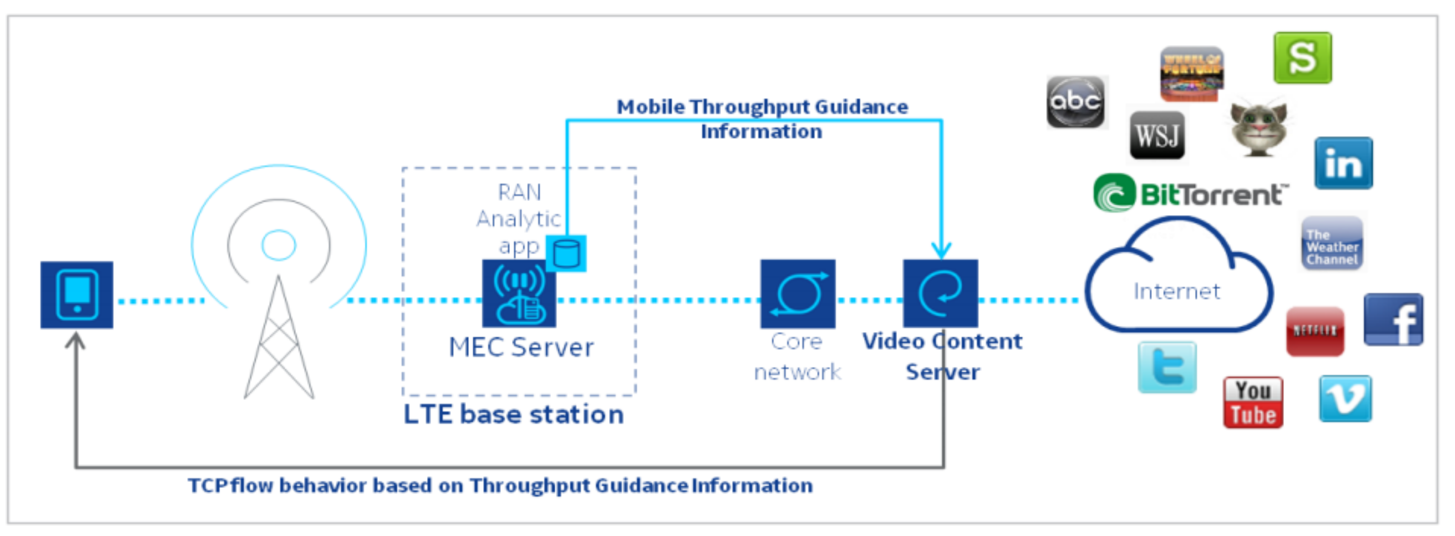
- This is based on the deployment of MEC (virtualization) servers, at multiple locations at the edge of the mobile network

- Some deployment locations are, for instance:
  - LTE/5G base stations (eNodeB)
  - 3G Radio Network Controllers (RNC)
  - cell aggregation sites (3G/LTE/WLAN - multi-Radio Access Technology)

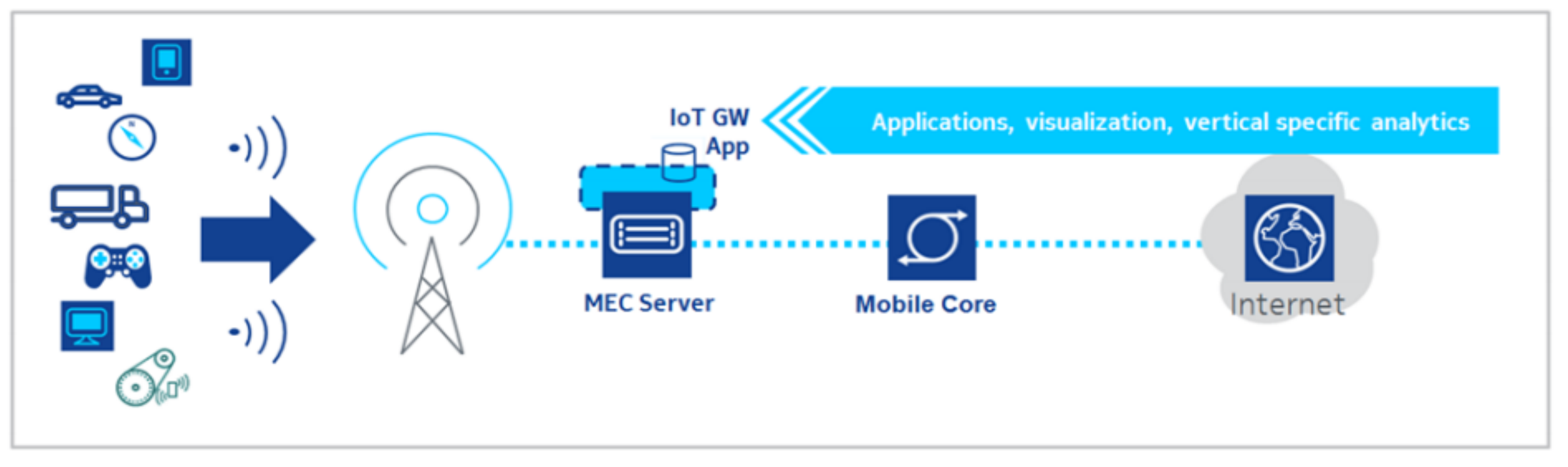


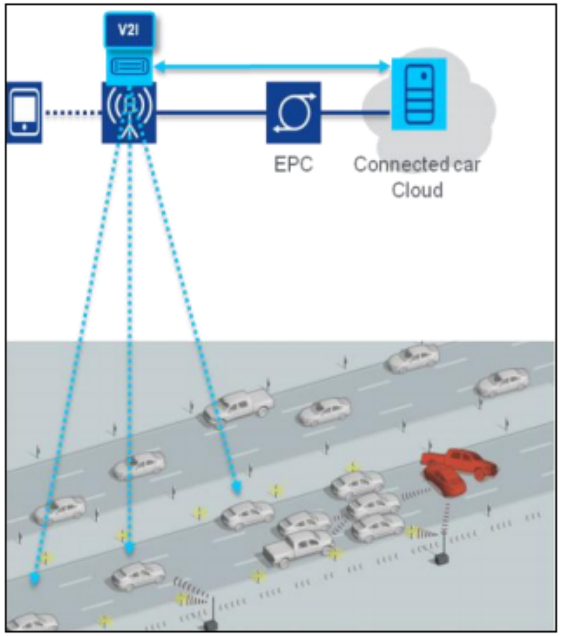
MEC – Use Cases





MEC – Use Cases

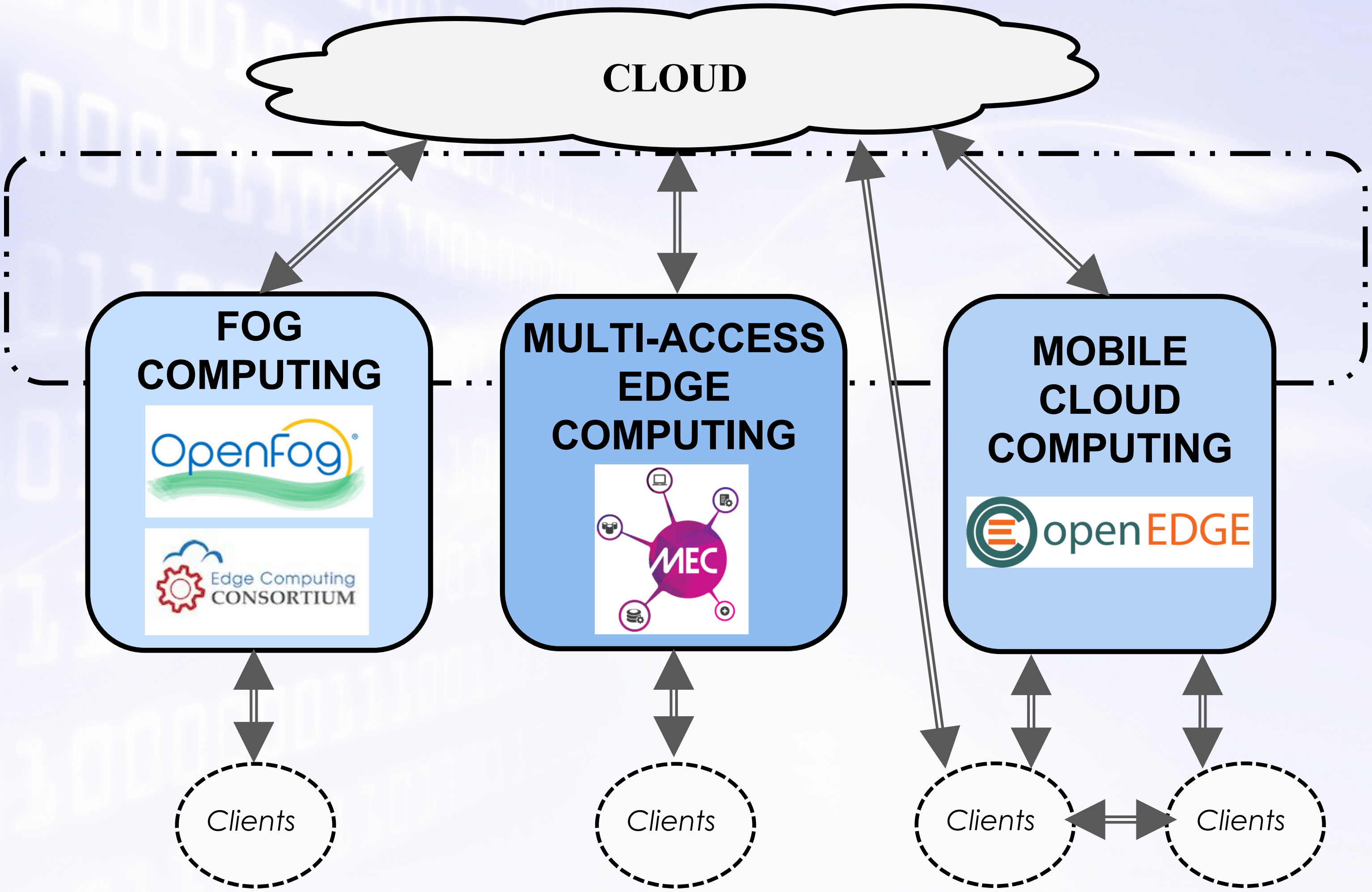




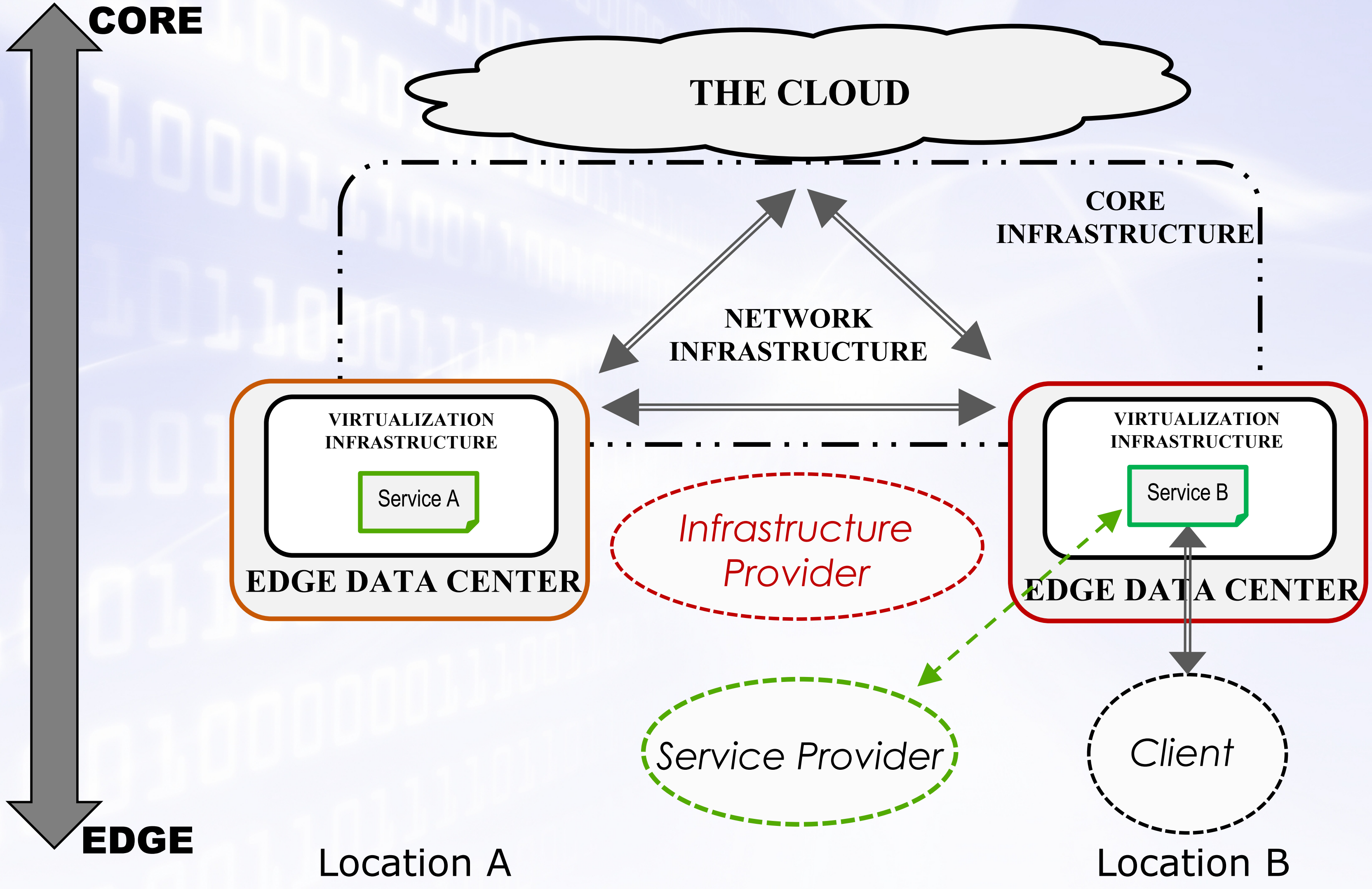
Multi-Access Edge Computing (MEC)

- The virtualization infrastructure is conceived to host not only MEC services, but also related services, like SDN and NFV
  - providing a common management and orchestration infrastructure
- In essence, mobile network operators want to optimize their existing mobile infrastructure services
  - though deployment of services will not be limited to them; also opened to third party service providers
    - creating an open ecosystem, where service providers can deploy their applications across multi-vendor MEC platforms
- MEC represents a key technology and architectural concept to enable the evolution to 5G

The three paradigms

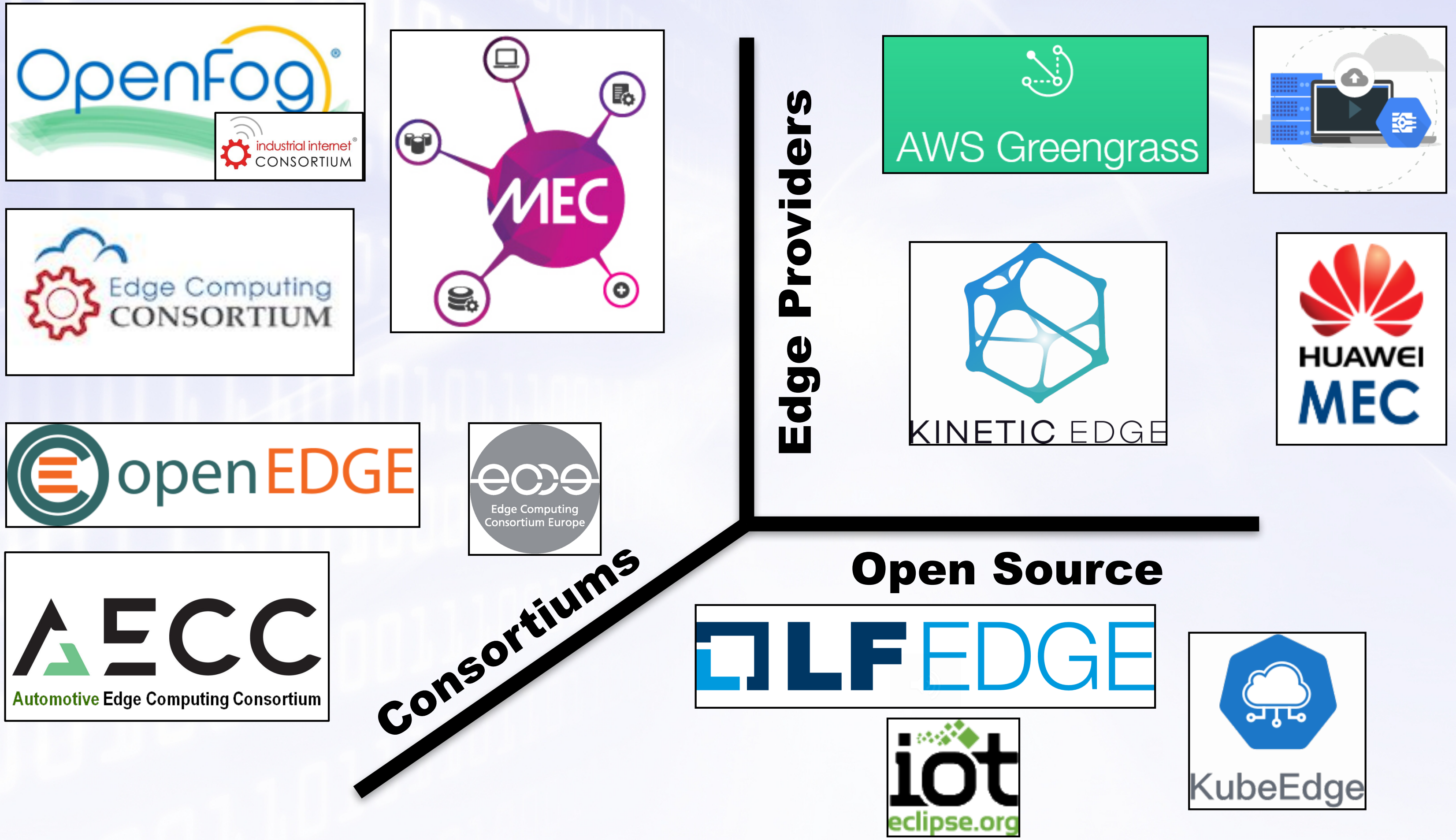


Edge Computing



The Ecosystem

Edge Computing: Present and Future



Edge Providers

Open Source

Consortiums

OpenFog

industrial internet CONSORTIUM

MEC

Edge Computing CONSORTIUM

openEDGE

Edge Computing Consortium Europe

AECC

Automotive Edge Computing Consortium

AWS Greengrass

KINETIC EDGE

HUAWEI MEC

LF EDGE

iot eclipse.org

KubeEdge

Consortiums: Multi-Access Edge Computing (MEC)

Accelleran
ACS
ADVA Optical Networking SE
Akamai Technologies
Altiostar
Artesyn Embedded Computing Inc.
ASTRI
AT&T GNS Belgium SPRL
Ceragon Networks AS
China Mobile Research Inst.
CPLANE NETWORKS, Inc.
DELL Inc.
ETRI
EURECOM
FUJITSU Laboratories of Europe
GSMA Association
Hewlett-Packard Enterprise

ICS
Intel Corporation (UK) Ltd
InterDigital, Inc.
INTRACOM TELECOM SOLUTIONS SA
IPGallery
ISMB
ITRI
Ixia Technologies
Juniper Networks
KDDI Corporation
MeadowCom
Motorola Mobility UK Ltd.
NEC EUROPE LTD
Netas
Netrounds
Nokia Germany
Openet Telecom

PT Portugal SGPS SA
Quortus Limited
Saguna Networks Ltd
Samsung R&D Institute UK
SCILD Innovations
Sony Europe Limited
Tech Mahindra Ltd
Telenity
TNO
Tseng InfoServ, LLC
TURK TELEKOMUNIKASYON A.S.
University Carlos III de Madrid
Vasona Networks Inc
ViaviSolutions Deutsch GmbH
Virtuosys Limited
…and others…

Consortiums: OpenFog

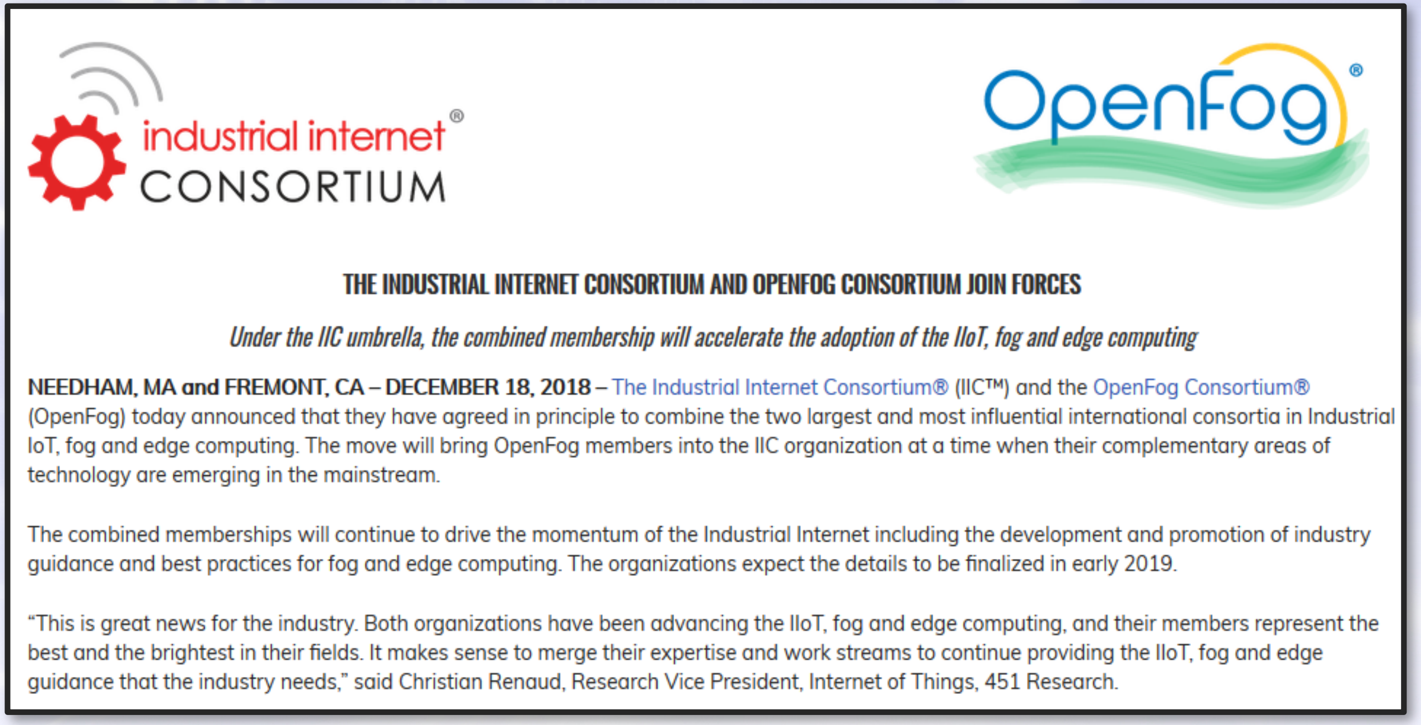
OpenFog™
ARM®
cisco™
DELL
intel®
at&t
Microsoft
FOXCONN®
HITACHI
TOSHIBA
FUJITSU

Aalto University
ABBALab inc.
AetherWorks, LLC.
Arizona State University
Caltech
Denver South Economic Development Partnership
FogHorn Systems
Incheon National University
Industrial Technology Research Institute (ITRI)
Institute for Information Industry
Institute of Network Coding, The Chinese University of Hong Kong

Internet Initiative Japan Inc.
ITOCHU techno-Solutions Corporation
Kii
LGS Innovations
MARSEC
Mitsubishi Electric Corporation
National Chiao Tung University
National Taiwan University
Nebbiolo Technologies
NGD Systems, Inc.
NTT Communications
OSIsoft LLC
Princeton University
PrismTech
Real-Time Innovations
relayr Inc

SAKURA Internet
Schneider Electric
Sensify Security
Shanghai Institute of Microsystem and Information Technology
ShanghaiTech University
Singapore University of Technology and Design
Stichting imec Nederland
The Chinese University of Hong Kong
Technische Universität Dresden
TTTech
Vanderbilt University
Wayne State University
ZTE Corporation
…and others…

Consortiums: OpenFog ⊂ Industrial Internet



industrial internet® CONSORTIUM

OpenFog®

THE INDUSTRIAL INTERNET CONSORTIUM AND OPENFOG CONSORTIUM JOIN FORCES

Under the IIC umbrella, the combined membership will accelerate the adoption of the IIoT, fog and edge computing

NEEDHAM, MA and FREMONT, CA – DECEMBER 18, 2018 – The Industrial Internet Consortium® (IIC™) and the OpenFog Consortium® (OpenFog) today announced that they have agreed in principle to combine the two largest and most influential international consortia in Industrial IoT, fog and edge computing. The move will bring OpenFog members into the IIC organization at a time when their complementary areas of technology are emerging in the mainstream.

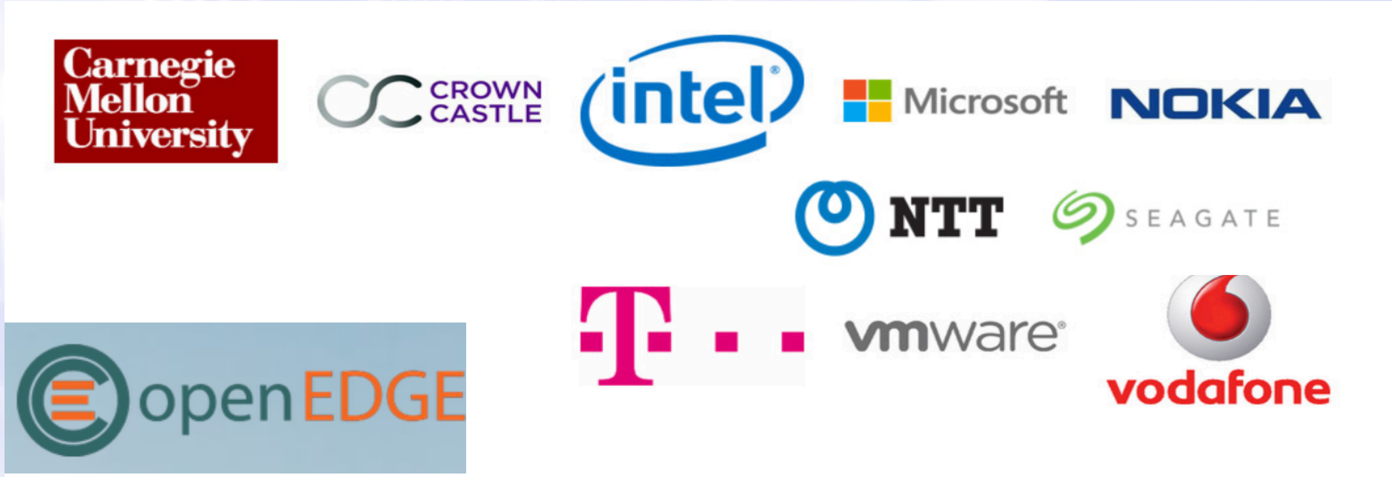
The combined memberships will continue to drive the momentum of the Industrial Internet including the development and promotion of industry guidance and best practices for fog and edge computing. The organizations expect the details to be finalized in early 2019.

"This is great news for the industry. Both organizations have been advancing the IIoT, fog and edge computing, and their members represent the best and the brightest in their fields. It makes sense to merge their expertise and work streams to continue providing the IIoT, fog and edge guidance that the industry needs," said Christian Renaud, Research Vice President, Internet of Things, 451 Research.

ABB BOSCH Invented for life DELL EMC FUJITSU GE

HUAWEI Microsoft MITRE PURDUE UNIVERSITY College of Engineering rti Your systems. Working as one.

Consortiums: OpenEdge and others



- Edge Computing Consortium (Europe)
  - *GOAL*: Explore the deployment of *distributed open platforms at the network edge*
  - Focusing on *China* and *Europe*
- Automotive Edge Computing Consortium
  - Analyze how the Edge can *cope with the needs of the future automotive services*

Edge Providers

- The world's top cloud computing providers are starting to move solutions to the Edge
  - Amazon
    - AWS Greengrass
  - Microsoft
    - Azure IoT Edge
  - Google
    - Google Cloud IoT Edge
    - Edge TPU chip for edge devices
  - IBM
    - No specific solution for Edge yet

- Some of these solutions are open-source

Edge Providers

- Not only Cloud providers are moving to the network Edge…
  - Telco-providers are providing software platforms both for supporting 5G as well as more general purpose edge computing
    - Nokia Mobile Edge Computing
    - Ericsson Edge NFVI, Edge Gravity
    - SK Telecom 5G MEC Open platform
    - Huawei MEC@CloudEdge
  - Other companies are providing both software and hardware
    - Vapor Kinetic Edge
    - MobiledgeX Edge-Cloud & Cloudlets
    - Cyrus™ by ASOCS
    - Dell Edge Gateways
    - Cisco Kinetic EFM,
    - Nebbiolo Technologies, …

Open Source Initiatives

- There is also a growing number of open source projects trying to accelerate the deployment of edge computing

- Some of the most important developments are being pushed by relevant foundations and corporations
  - The Linux Foundation
  - Eclipse Foundation
  - OpenStack Foundation
  - Huawei
  - Baidu
  - Microsoft …

Open Source Initiatives

- The Linux Foundation has created LF Edge to develop a unified open source framework for edge computing

- LF Edge includes various projects:
  - Akraino Edge Stack software stack that supports high-availability cloud services optimized for edge computing
  - EdgeX Foundry microservices framework that provides the choice to plug and play from applications with a focus on IoT Edge
  - Home Edge Project, concentrates on enabling a robust, reliable, and intelligent home edge computing framework (no code available yet)
  - Project EVE, develops the open source Edge Virtualization Engine capable of deploying applications on bare metal hardware

AKRAINO EDGE STACK

HOME EDGE

EDGE VIRTUALIZATION ENGINE

EDGEXFOUNDRY™

NICS

Open Source Initiatives

- The Eclipse Foundation is working on a number of projects with Eclipse IoT for enabling the IoT
  - Each project is focused on a particular problem, hence any solution may need to rely on several of them
- Among the various Eclipse IoT projects there are two particularly focussed on edge computing
  - Eclipse ioFog, edge computing platform to build and run applications at the edge
  - Eclipse Fog Ø5, aims to provide a virtualised infrastructure compatible with ETSI MEC (just approved, no code available)
- Both projects are still in incubation phase

Open Source Initiatives

- The OpenStack foundation is aimed at developing open source software for creating private and public clouds

- The Starling X project built on top of an OpenStack configuration with other technologies such as QEMU and Kubernetes

STARLINGX

- The StarlingX is designed with 5G and Industrial automation in mind so they are focussing on providing
  - High availability
  - Quality of Service
  - Low latency
  - Rapid response to events

Open Source Initiatives

- Some private companies are also involved in open source initiatives:
  - Huawei KubeEdge: platform based on Kubernetes for application orchestration at the network edge
  - Baidu OpenEdge: open source version of commercial Baidu Intelligent Edge to extend cloud computing data and services to the Edge
  - Microsoft Azure IoT Edge: builds on top of Azure IoT Hub with the goal of providing data analytics at the edge

KubeEdge

OpenEdge

Azure IoT Edge

EU-Funded Projects

- FOGHORN (FOG-aided wireless networks for communication, cacHing and cOmputing: theoRetical and algorithmic fouNdations) [ERC-COG: Jun17-May22]
  - Develop fundamental theoretical and algorithmic foundations of fog-aided wireless networks
    - Overall budget: € 2.318.719
- PrEstoCloud (Proactive Cloud Resources Management at the Edge for Efficient Real-Time Big Data Processing) [RIA: Jan17-Dec19]
  - Provide a dynamic, self-adaptive and proactively configurable architecture for processing Big Data streams in a Cloud-Edge scenario.
    - Overall budget: € 4.256.502,50
- mF2C (Towards an Open, Secure, Decentralized and Coordinated Fog-to-Cloud Management Ecosystem) [RIA: Jan17-Dec19]
  - designing an open, secure, decentralized, multi-stakeholder management framework for the Fog and Cloud continuum.
    - Overall budget: € 5.440.287,50

EU-Funded Projects

- FAR-EDGE (Factory Automation Edge Computing Operating System Reference Implementation) [RIA: Oct16-Sep19]
  - Novel factory automation platform based on edge computing architectures and IoT/CPS technologies.
    - Overall budget: € 4.490.193,75

- LightKone (Lightweight Computation for Networks at the Edge) [RIA: Jan17-Dec19]
  - Development of a scientifically sound model for doing general-purpose computation on edge networks
    - Overall budget: € 3.570.993,75

- SESAME (Small cEllS coordinAtion for Multi-tenancy and Edge services) [RIA: July15-Dec17]
  - Placement of intelligence and applications in 5G networks through Network Functions Virtualisation (NFV) and Edge Cloud Computing
    - Overall budget: € 8.266.932,76

EU-Funded Projects

- 5GCity [IA: Jun17-Nov19]
  - Deploy a distributed cloud and radio platform for municipalities and infrastructure owners acting as 5G neutral hosts.
    - Overall budget: € € 7.720.001,13
- BigClouT (Big Data meeting Cloud and IoT for empowering the citizen clout in smart cities) [RIA: Jul16-Jun19]
  - Deployment of edge computing for creating distributed intelligence that can be used by city actors.
    - Overall budget: € 1.349.622,50

EU-Funded Projects

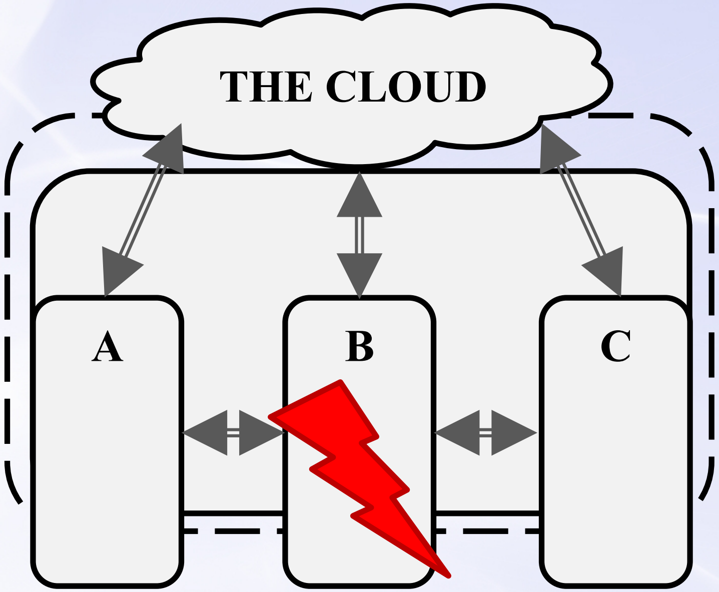
- ANASTACIA (Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures) [RIA: Jan17-Dec19]
  - Discovery of vulnerabilities in CPS/IoT architectures using Edge computing as a use case scenario.
    - Overall budget: € 5.420.208,75

- SECURED (SECURity at the network EDge) [FP7-CP: Oct13-Sept16]
  - Protection from Internet threats by offloading execution of security applications into trusted virtualized execution environments on network edge devices
    - Overall budget: € 4.131.724

SECURITY THREATS AND MECHANISMS

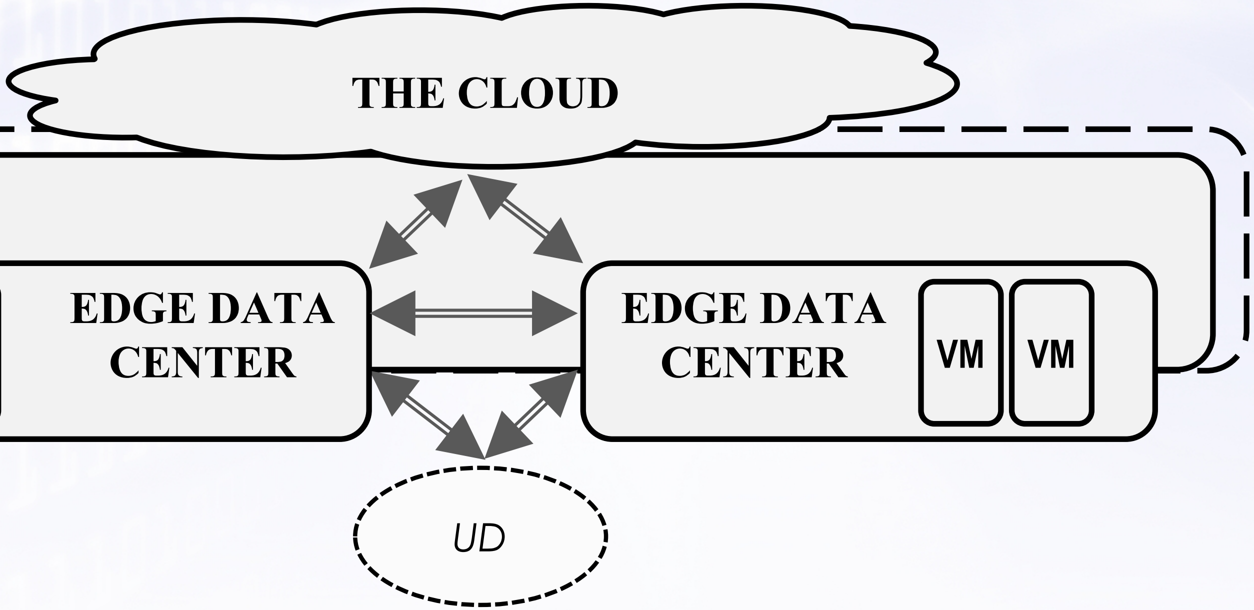
Security Threats

- There are various intrinsic aspects that must be considered when analyzing the security threats:
  - Lack of "global" perimeter: no single owner; ecosystem controlled by different actors that must cooperate
  - "Anything, anytime": attacks are very localized, and their impact is (usually) limited to a geographical location
    - As with the Internet, an attacker might control a portion of the infrastructure but not others
  - Multiple attacker profiles: external, internal, rogue elements,…



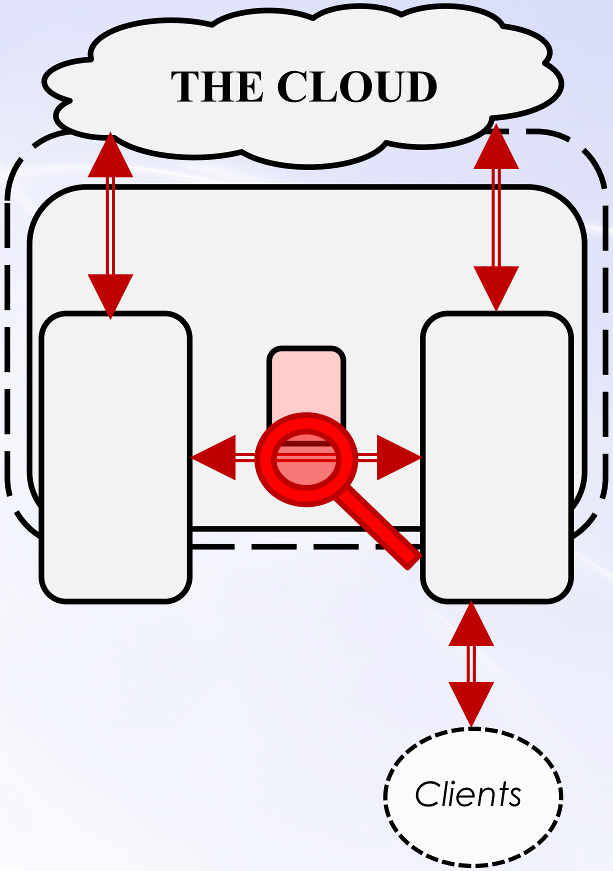
Security Threats – Generic Model

- We will follow an asset-based analysis, and show major security threats
  - A. Network Infrastructure: Communication networks
  - B. Edge Data Centers: Host virtualization, management, others
  - C. Core Infrastructure: mobile core networks, centralized clouds
  - D. Virtualization Infrastructure: virtualization services
  - E. User Devices: devices controlled by users



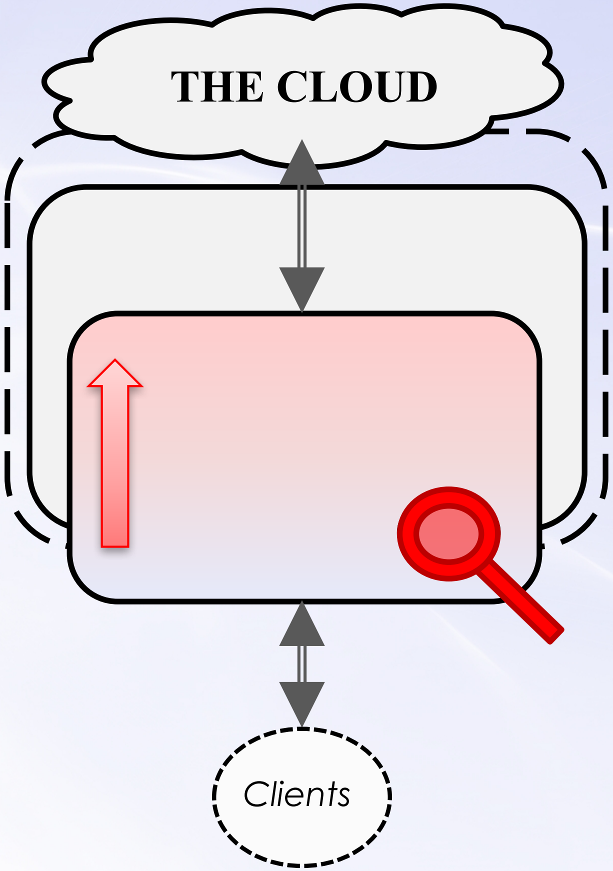
Threat Model: Network Infrastructure

- Denial of Service
  - Limited scope of the attack
  - Even weaker if autonomous security mechanisms are used in edge data centers
- Man in the Middle
  - Stealthy and dangerous, as it can affect all the information traversing that particular node
- Rogue gateway
  - Deployed by an adversary. Impact similar to MiM



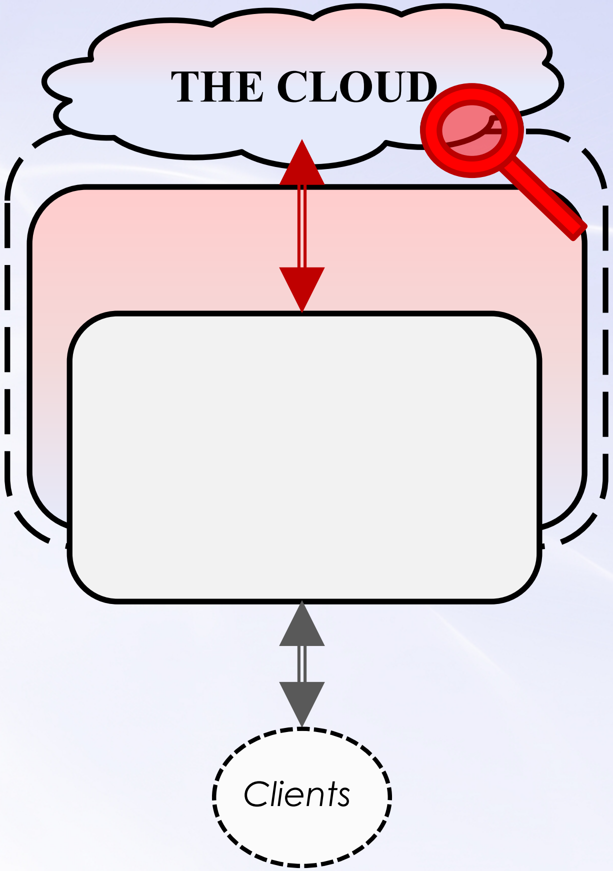
Threat Model: Edge Data Center

- Physical damage
  - Only if node is available and unprotected. Limited to a local scope.
- Privacy leakage
  - Internal adversaries access information flow that traverses the edge
- Privilege escalation
  - Incorrect maintenance or misconfiguration
- Service manipulation
  - By privilege escalation (selective DoS, selective information tampering, …)
- Rogue data center
  - Dangerous scenario!



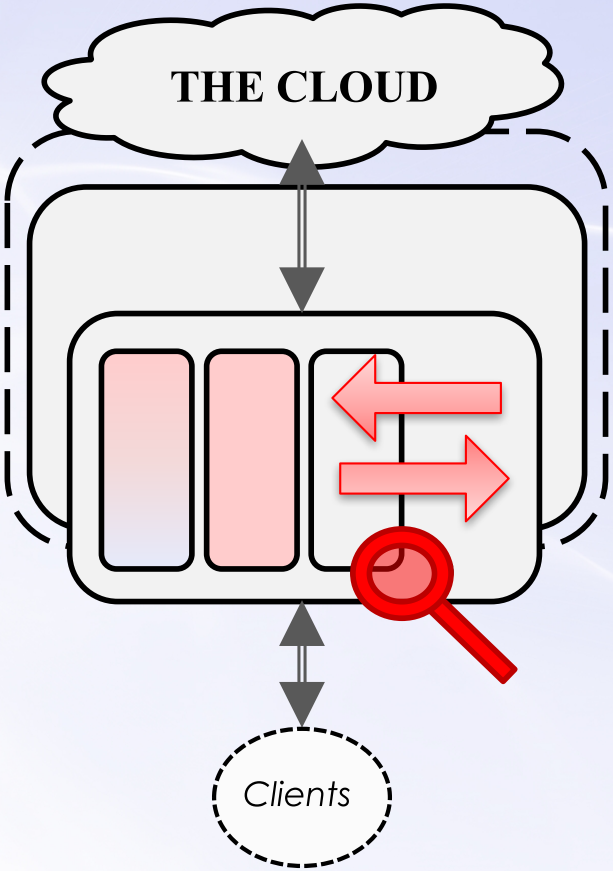
Threat Model: Core Infrastructures

- Privacy leakage
  - Information in upper layers may be accessed by unauthorized entities
  - Yet, scope is limited as some data is managed in lower layers
- Service manipulation
  - Adversary manipulates information flow, and also instantiate rogue services
  - Dangerous, yet whole ecosystem might not be affected due to distributed nature
- Rogue infrastructure
  - Mostly impractical, yet extremely dangerous



Threat Model: Virtualization Infrastructure

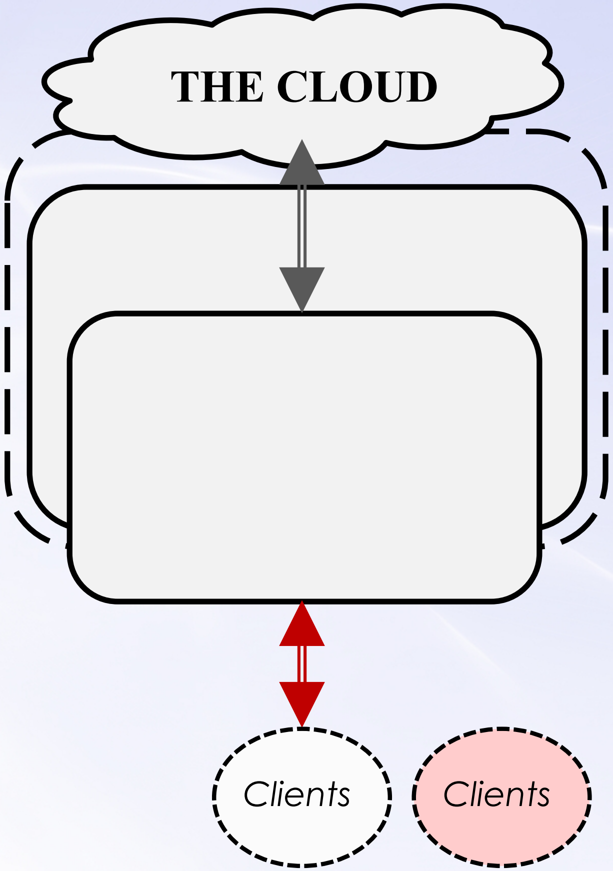
- Denial of Service
  - Malicious VM can try to deplete the resources of the node
- Misuse of resources
  - VMs searching for vulnerabilities in local context, running botnets
- Privacy leakage
  - VMs misusing the Virtualization Infrastructure APIs
- Privilege escalation
  - VMs abusing host vulnerabilities
- VM manipulation
  - Hosts manipulate VMs (extract information, load logic bombs)



Threat Model: User Devices

- Injection of Information
  - A device controlled by an adversary may distribute fake information

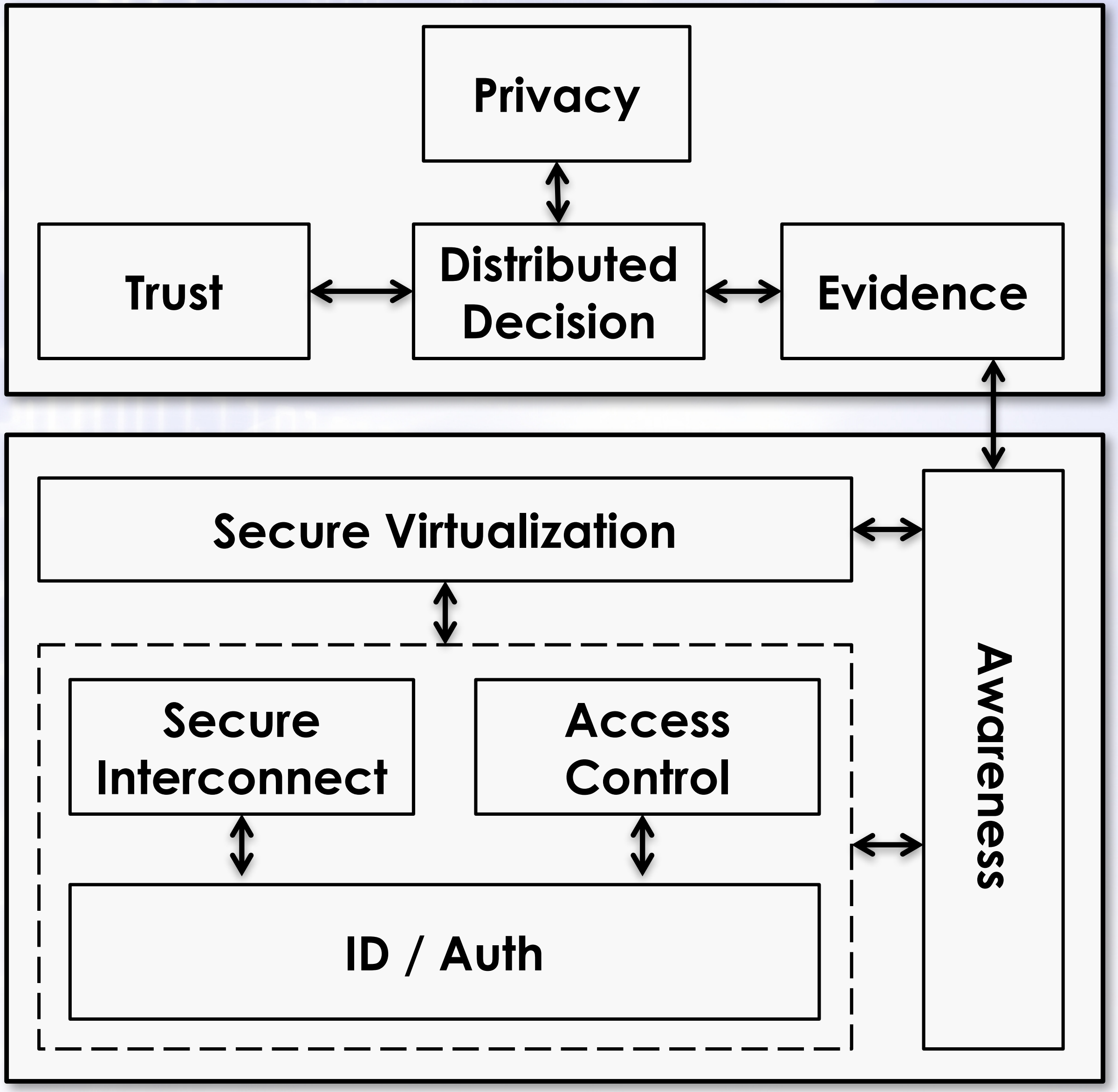
- Service manipulation
  - A device may participate (together with other devices) in the provisioning of services
    - For example, a cluster of devices with malicious entities



Security Threats – Influence of features

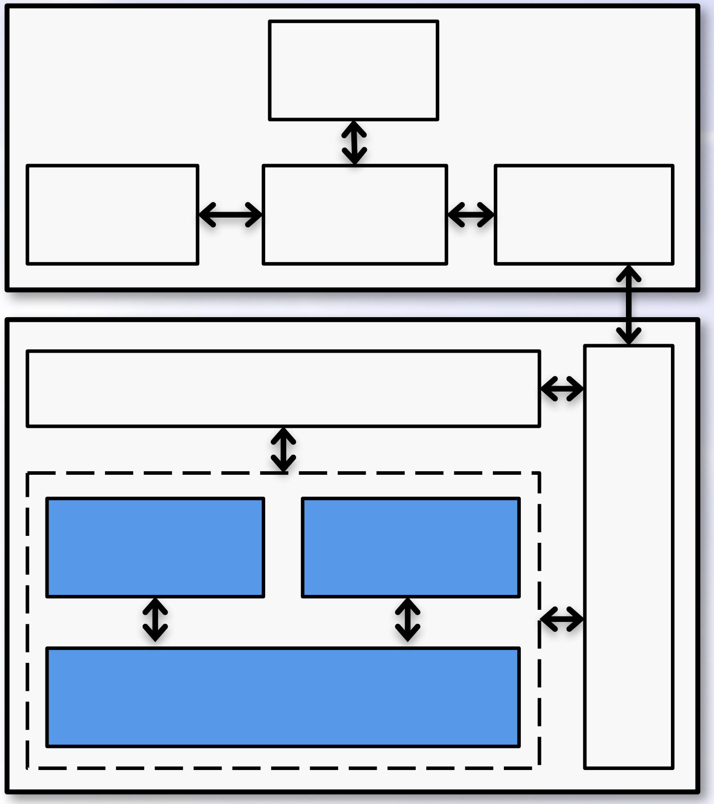
- How the features of different edge paradigms influence the security threats?
  - Ownership: Companies vs. SMEs / Users
    - Homogeneous vs. Heterogeneous ecosystem
    - Staff experience (system maintenance)
  - Hardware: Specialized, Commodity HW vs. μservers
    - HW Capabilities
    - Usage of HW extensions for virtualization
  - (deployment of) Services: Virtualization vs. others (clustering)
    - Additional issues caused by other service provisioning mechanisms
  - Network architecture: Centralization vs. Federation vs. Distribution
    - Different strategies have their own problems

Security Mechanisms



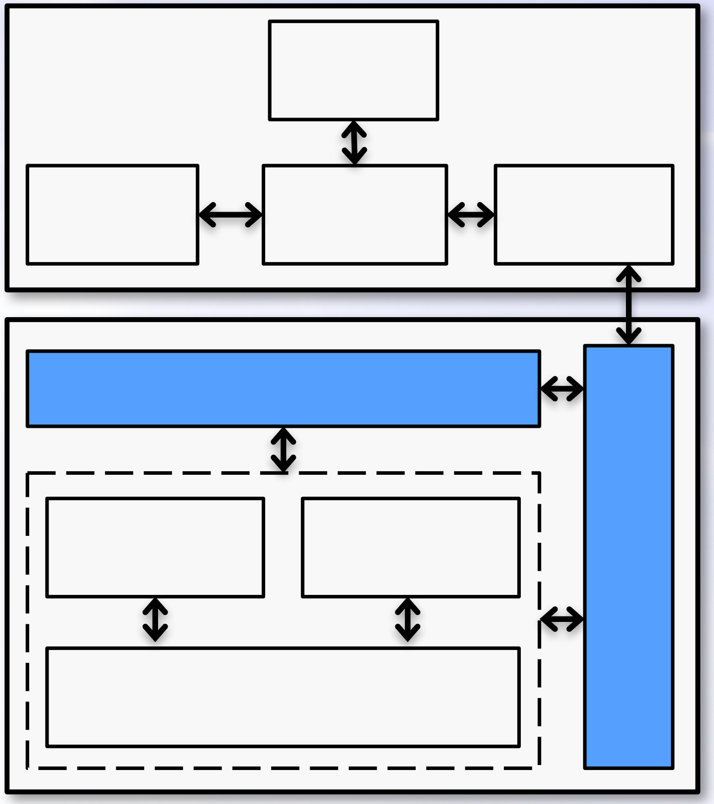
Security Mechanisms – Fundamental

- **ID / Auth**
  - All actors
    - Users
    - Service providers
    - Infrastructure providers
    - VMs…
- **Secure Interconnection**
  - Negotiate security parameters / credentials in heterogeneous environment
- **Access Control**
  - Heterogeneous context with different trust domains



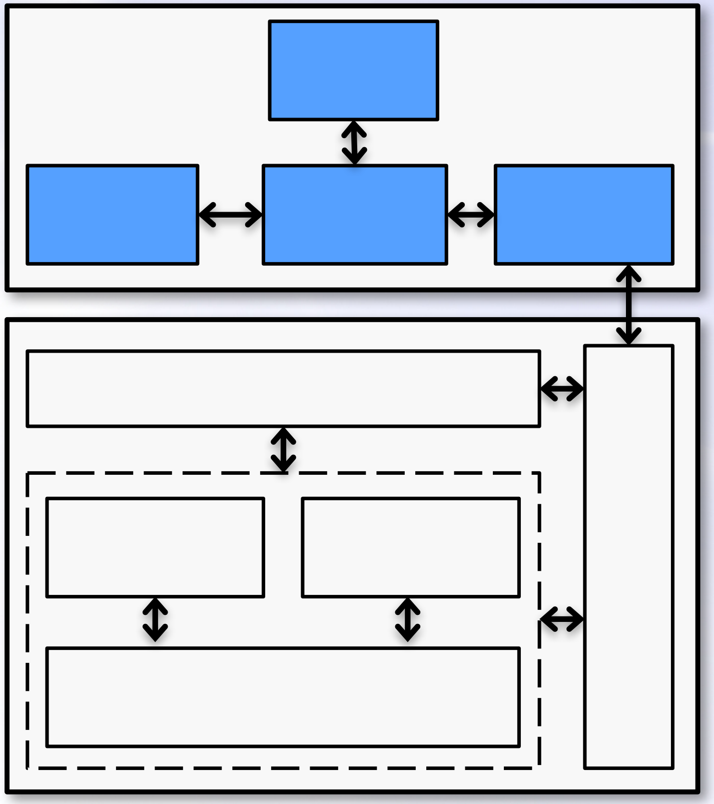
Security Mechanisms – Fundamental

- Secure Virtualization
  - Protect
    - …the edge node
    - …the VM itself and its lifecycle
- Awareness
  - Acquire status information of (all) interactions
    - Network
    - VM
    - Users
    - Administrators
    - …
  - Exchange this information between nodes and platforms



Security Mechanisms – Support

- Trust Services
  - "It is a wild world out there"
  - Support for interactions in presence of uncertainty
- Distributed Decision Making
  - Cryptographic mechanisms
    - Process encrypted data
    - Secure multiparty protocols
    - Distributed ledgers
- Privacy Support
  - Support
    - Mechanisms (PET)
    - Information
- Digital Evidence
  - Events as protected evidence



Security Mechanisms – Challenges

- Federated, distributed environment
  - Maintenance of distributed databases (IDS signatures)
  - Configuration of all elements
- Different trust domains
  - Interoperable mechanisms
- Coexistence of multiple actors, services, infrastructures
- Emphasis on geographical location
  - Specific policies based on location, other factors?
- Achieve a balance between Security & QoS

Outline

- **DAY 1**
  - Edge Computing Paradigm(s)
  - The Ecosystem
  - Security Threats and Mechanisms

- **DAY 2**
  - Main Edge Architectures: OpenFog and MEC
  - Security in OpenFog and MEC
  - Research on Edge Security Mechanisms
  - Edge Computing as a Security Enabler
  - Examples of Using the Edge for Enhanced Security

MAIN EDGE ARCHITECTURES: OPENFOG AND MEC

OpenFog Reference Architecture (IEEE 1934-2018)

OpenFog Consortium –

Industrial Internet Consortium

OpenFog Principles

- Conceived to support the (Industrial) Internet of Things. It aims to evolve and become:

A. Horizontal Architecture – *Cooperation & Interoperability*

  - *"Support multiple industry verticals and application domains, delivering intelligence and services to users and business"*

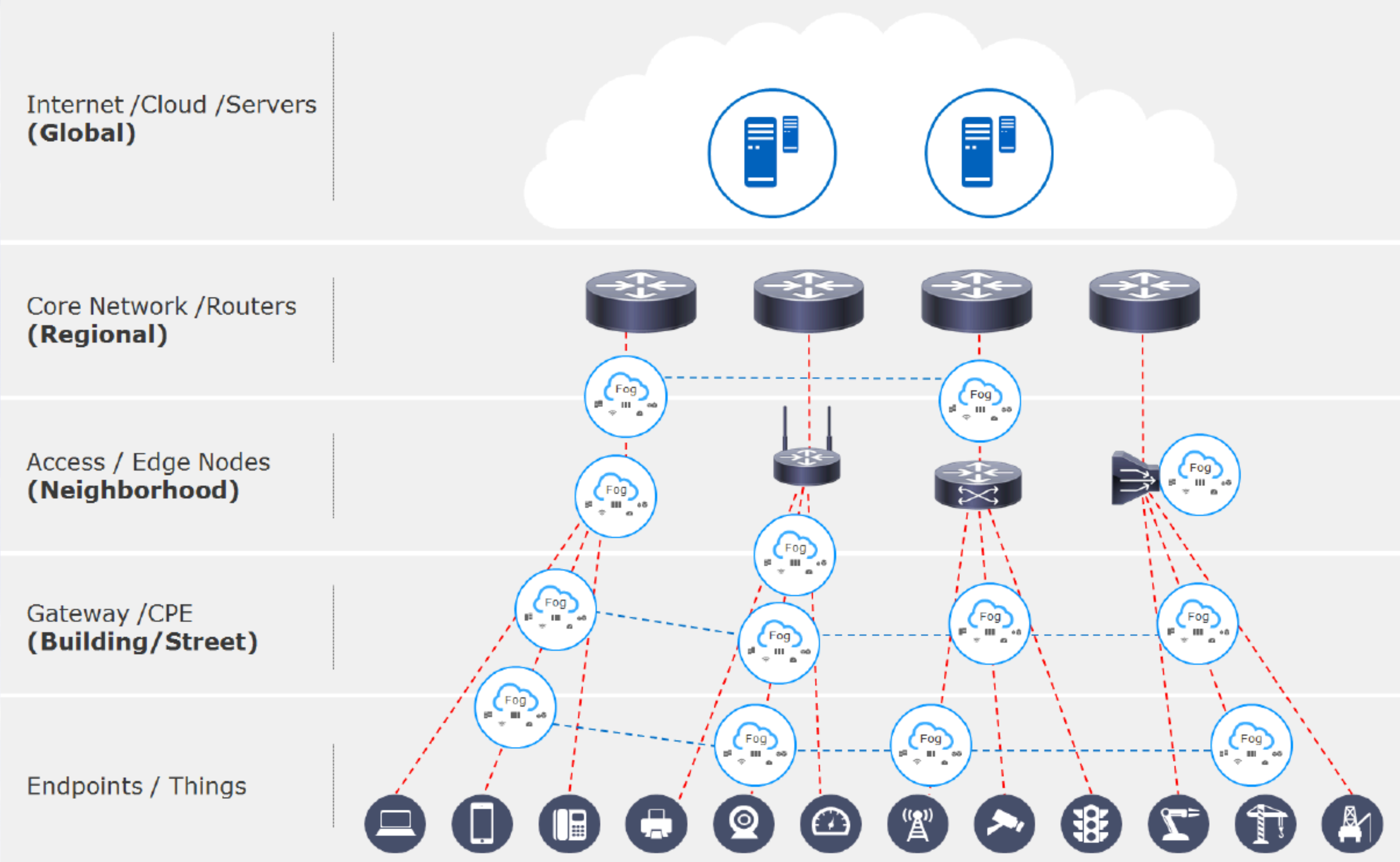
B. System-level – *Fog infrastructure in all layers*

  - *"Extend from the Things, over the network edges, through the Cloud, and across multiple protocol layers" – 'Holistic' perspective*

C. Cloud-to-Thing continuum of services – *Services in all layers*

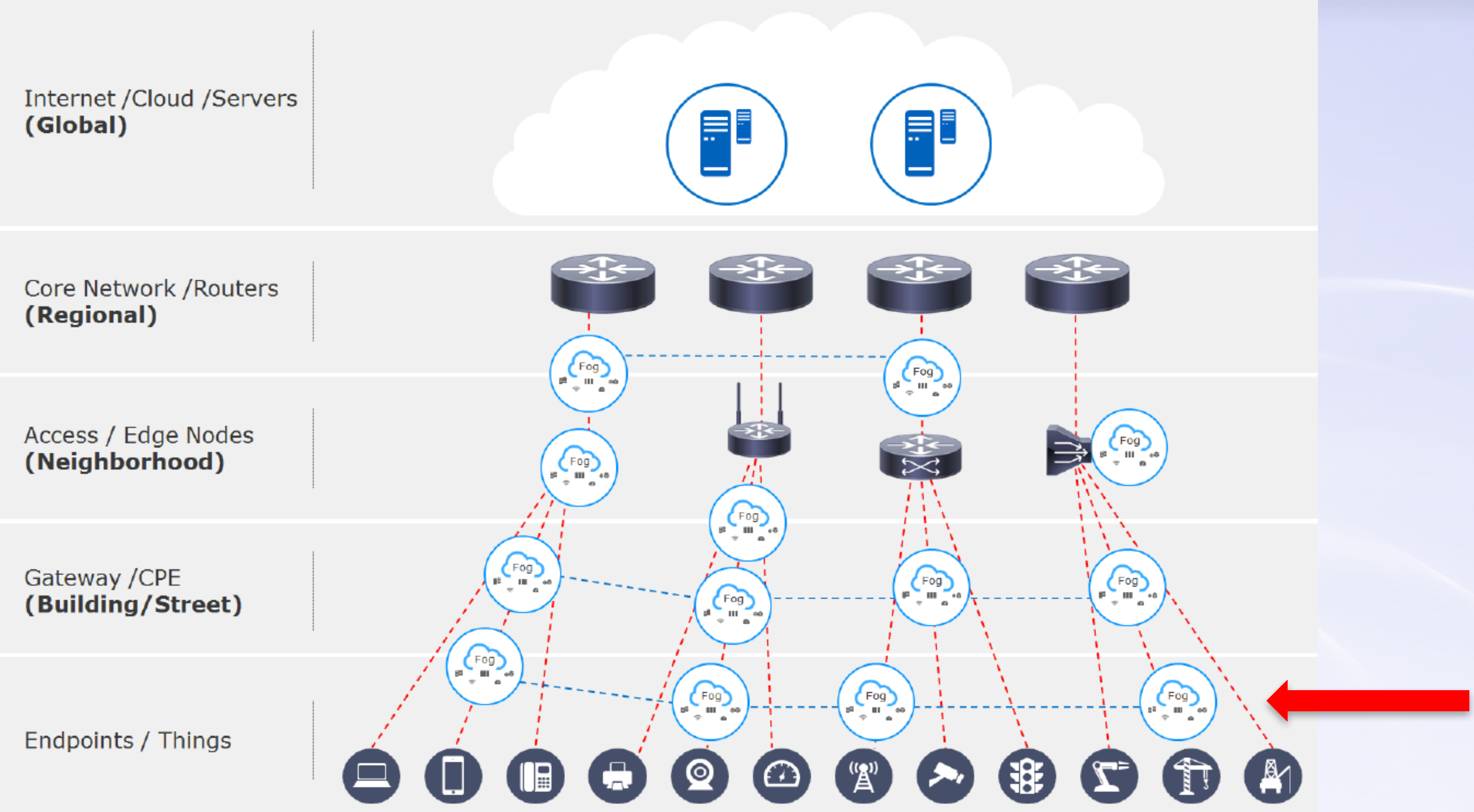
  - *"Enable services and applications to be distributed closer to Things, and anywhere along the continuum between Cloud and Things Multi-stakeholder (IT + others) initiative"*

OpenFog deployment: global picture



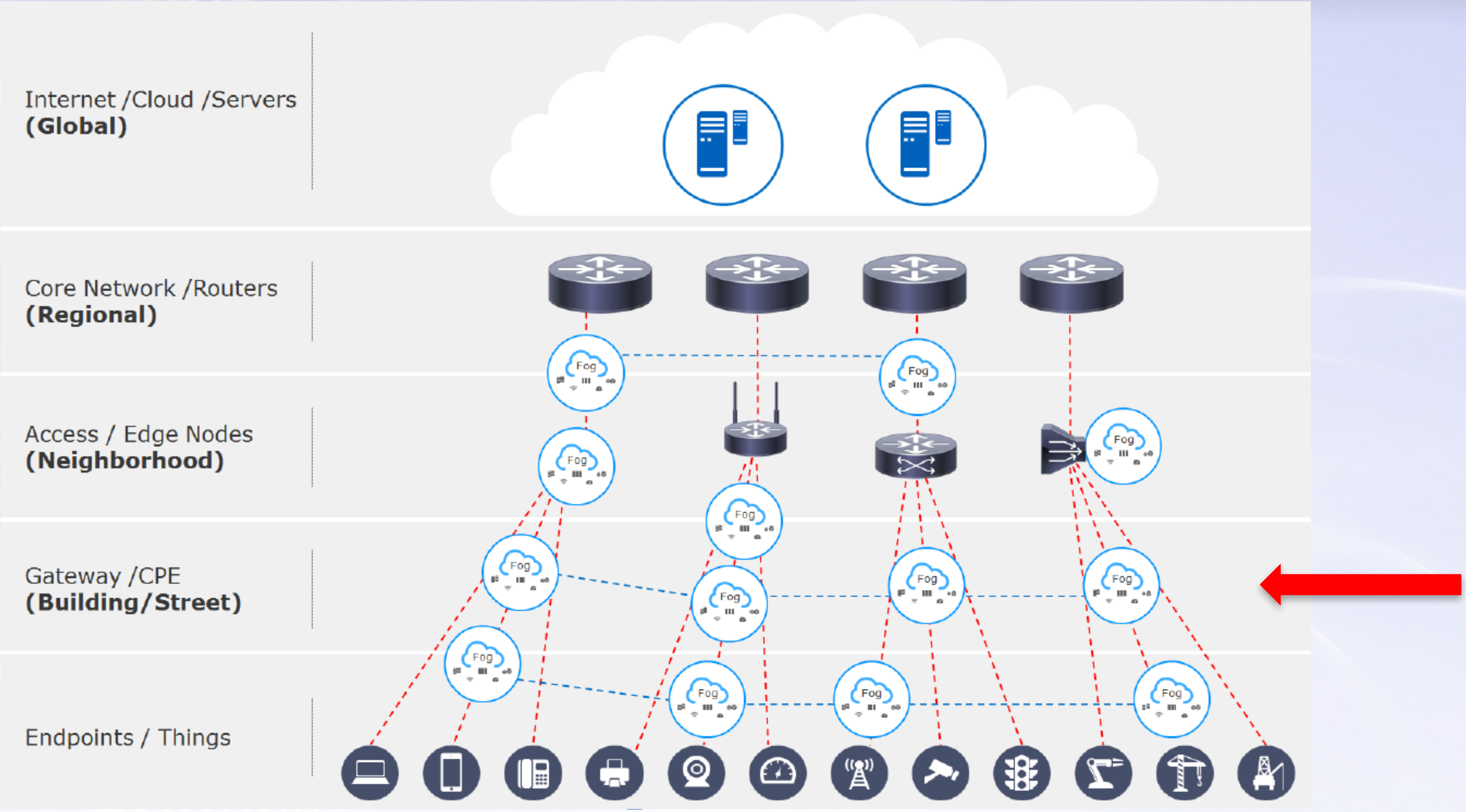
- Nodes form a mesh (communication up-down and laterally)
  - Better load balancing, resilience, fault tolerance, data sharing…

OpenFog deployment: global picture



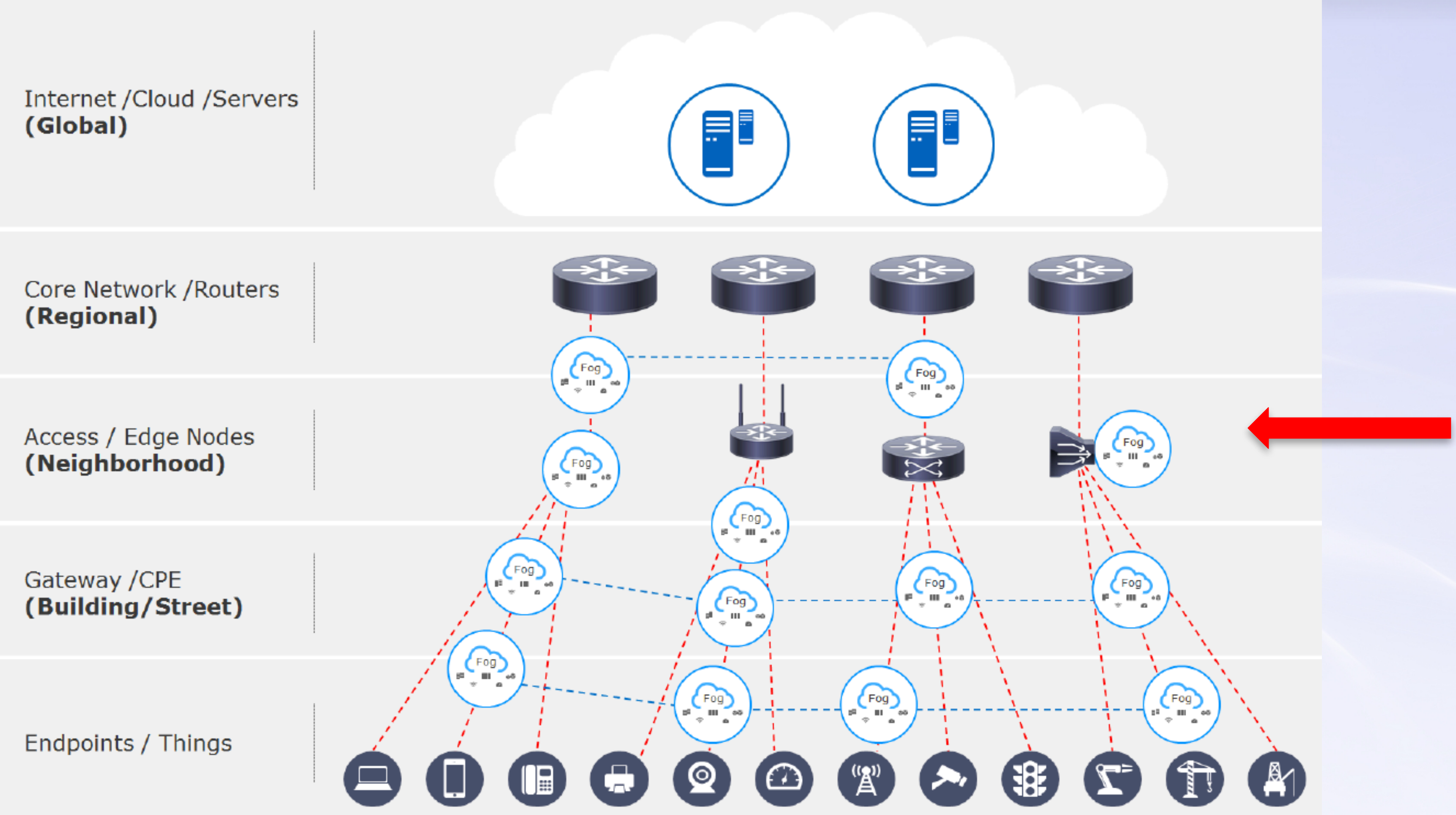
- Nodes at the edge are normally focused on sensor data acquisition, data normalization, and command/control of sensors and actuators.

OpenFog deployment: global picture



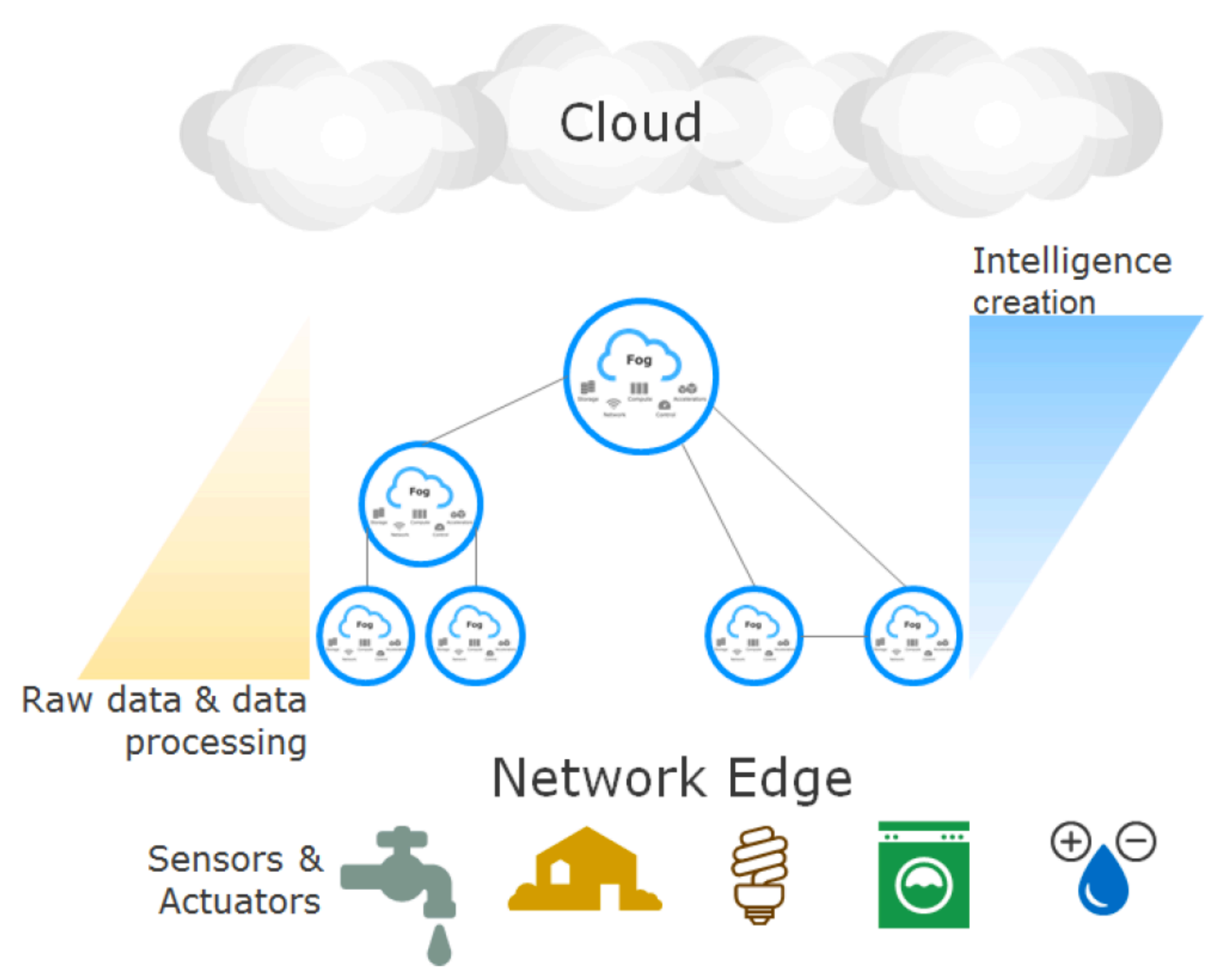
- Nodes in the next higher tier are focused on data filtering, compression, and transformation
  - may also provide some edge analytics for critical real time processing.

OpenFog deployment: global picture

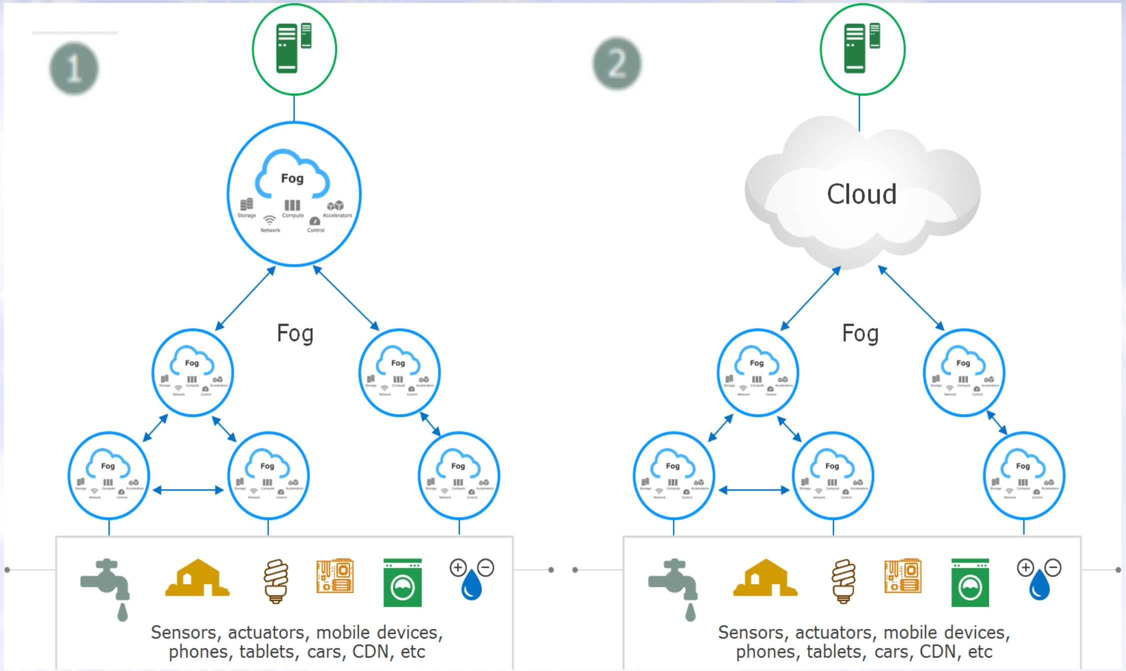


- Nodes at the higher tiers or nearest the backend cloud are typically focused on aggregating data and turning the data into knowledge

OpenFog deployment: global picture



OpenFog deployment: models

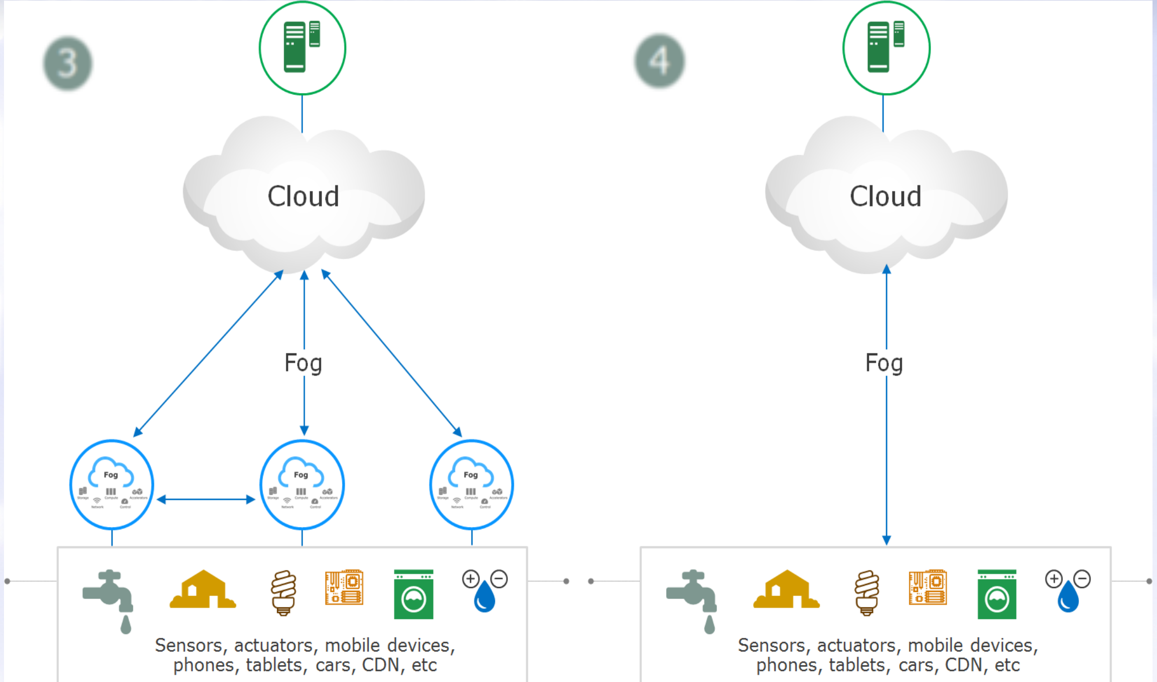


1
2
Fog
Cloud
Fog
Fog
Storage
Compute
Accelerators
Network
Control
Sensors, actuators, mobile devices, phones, tablets, cars, CDN, etc
Sensors, actuators, mobile devices, phones, tablets, cars, CDN, etc

1) Applicable in use cases when cloud can't be used:
   - event-to-action time window is very low
   - E.g.: armed forces combat systems, use of drones, healthcare systems, …

2) Cloud used for information processing related to decision making
   - event-to-action time window ranges from hours to days
   - E.g. commercial building management, retail, …

OpenFog deployment: models

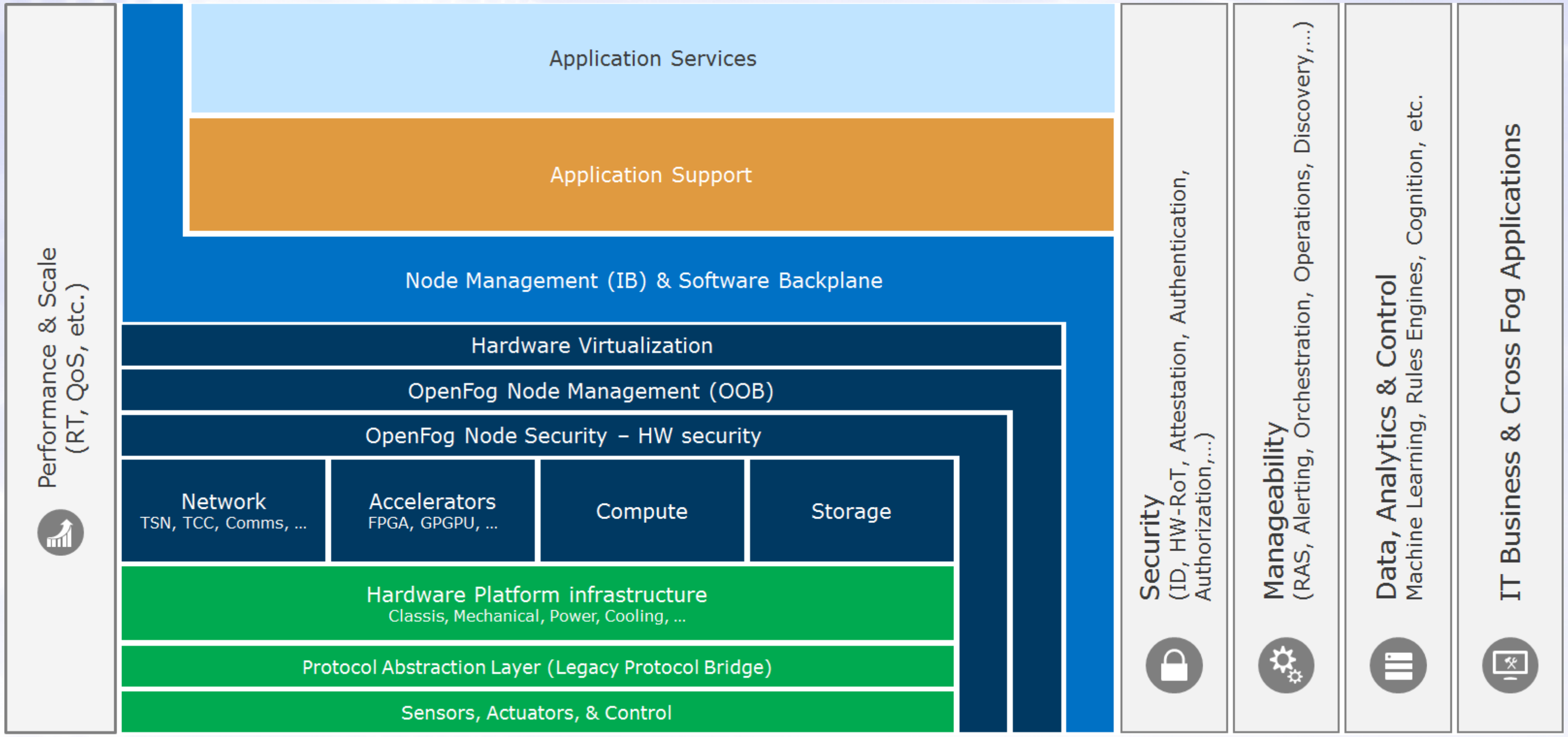

3
Cloud
Fog
Fog
Fog
Fog
Sensors, actuators, mobile devices, phones, tablets, cars, CDN, etc
4
Cloud
Fog
Sensors, actuators, mobile devices, phones, tablets, cars, CDN, etc

3. Local fog infrastructure used for time-sensitive computation
   - … while cloud used for business-related information processing.
   - E.g.: UPS device monitoring, content delivery networks (CDNs), …

4. Deployment of fog may not be feasible or economical.
   - Fog nodes at the device layer may get some monitoring/control function
   - E.g.: Agriculture, remote weather stations, …

OpenFog – Reference Architecture (RA)

- Architecture: Composition of Views / Perspectives
  - **View**: Representation of one or more structural aspects of the architecture
  - **Perspective**: Cross-cutting concern of the architecture



Performance & Scale
(RT, QoS, etc.)

Application Services

Application Support

Node Management (IB) & Software Backplane

Hardware Virtualization

OpenFog Node Management (OOB)

OpenFog Node Security – HW security

Network
TSN, TCC, Comms, ...

Accelerators
FPGA, GPGPU, ...

Compute

Storage

Hardware Platform infrastructure
Classis, Mechanical, Power, Cooling, ...

Protocol Abstraction Layer (Legacy Protocol Bridge)

Sensors, Actuators, & Control

Security
(ID, HW-RoT, Attestation, Authentication, Authorization,...)

Manageability
(RAS, Alerting, Orchestration, Operations, Discovery,...)

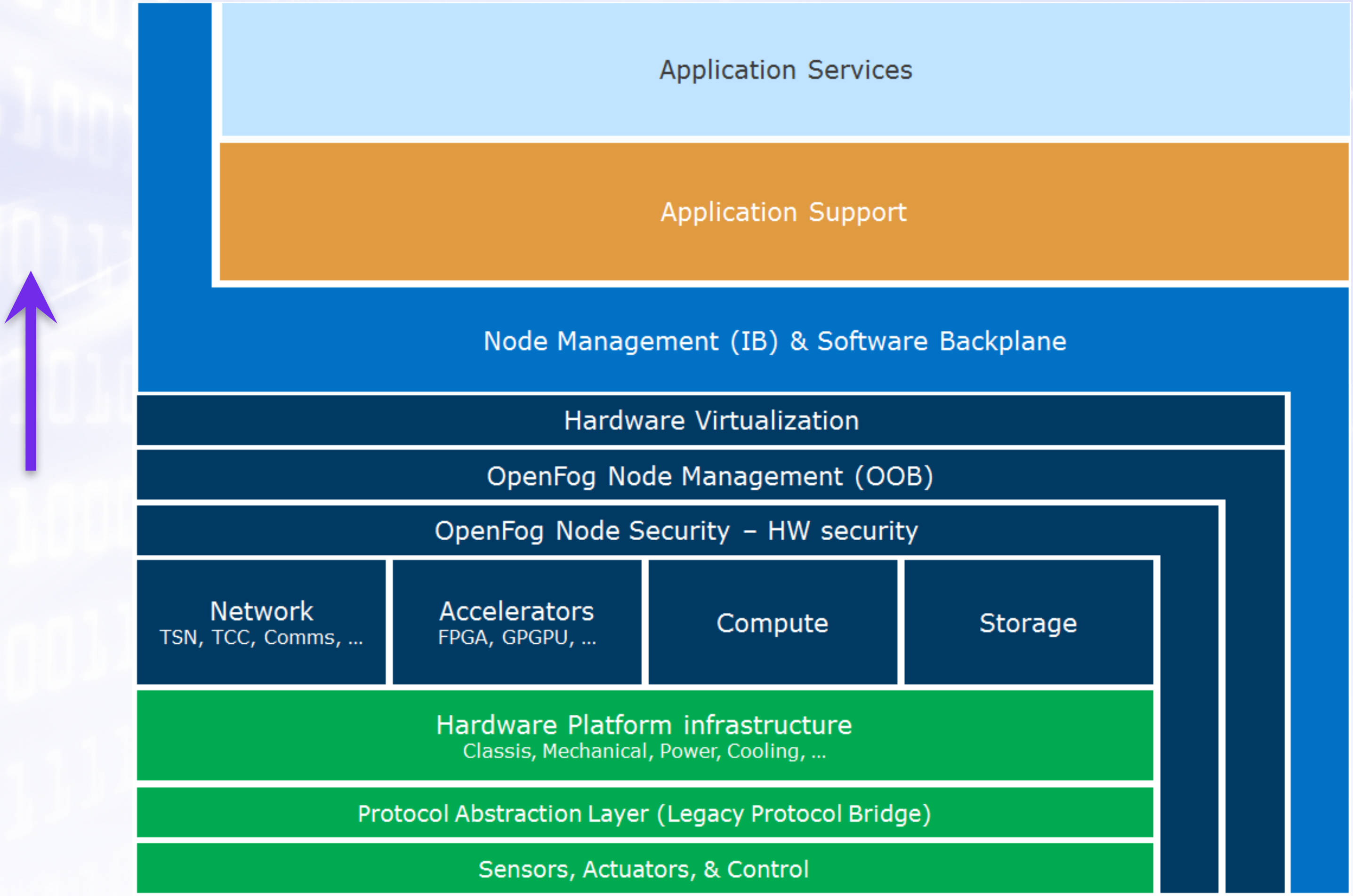
Data, Analytics & Control
Machine Learning, Rules Engines, Cognition, etc.

IT Business & Cross Fog Applications

- NOTE: Document mostly provides functional and deployment analyses
  - Requirements, potential components and their interactions…

OpenFog – Architecture: Views

- Views:
  - **Software**
  - **System**
  - **Node**

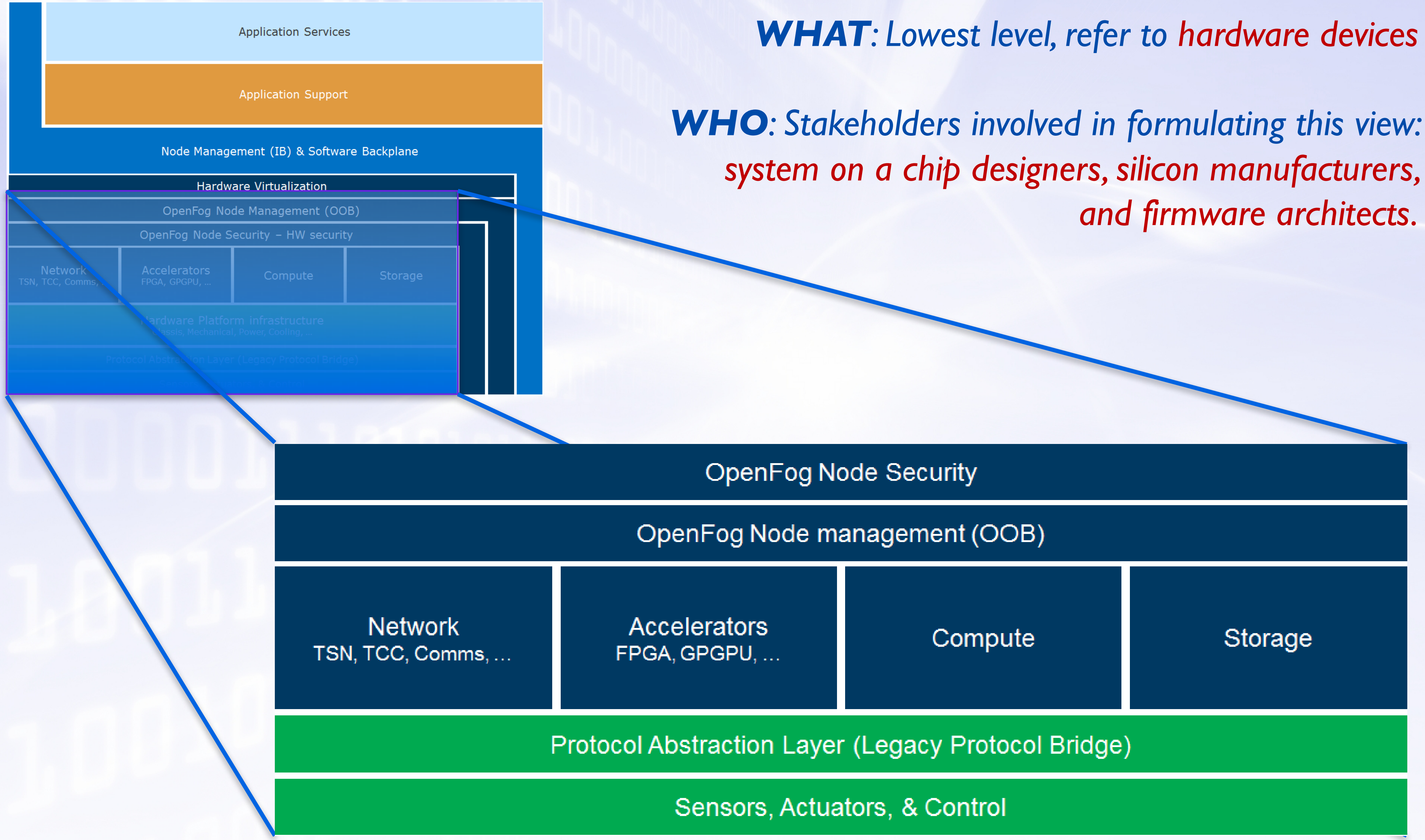


Application Services
Application Support
Node Management (IB) & Software Backplane
Hardware Virtualization
OpenFog Node Management (OOB)
OpenFog Node Security – HW security
Network
TSN, TCC, Comms, ...
Accelerators
FPGA, GPGPU, ...
Compute
Storage
Hardware Platform infrastructure
Classis, Mechanical, Power, Cooling, ...
Protocol Abstraction Layer (Legacy Protocol Bridge)
Sensors, Actuators, & Control

OpenFog – View: Nodes

***WHAT**: Lowest level, refer to hardware devices*

***WHO**: Stakeholders involved in formulating this view: system on a chip designers, silicon manufacturers, and firmware architects.*



Application Services

Application Support

Node Management (IB) & Software Backplane

Hardware Virtualization

OpenFog Node Management (OOB)

OpenFog Node Security – HW security

Network
TSN, TCC, Comms, … | Accelerators
FPGA, GPGPU, … | Compute | Storage

Hardware Platform infrastructure
Chassis, Mechanical, Power, Cooling, …

Protocol Abstraction Layer (Legacy Protocol Bridge)

Sensors, Actuators, & Control

OpenFog Node Security

OpenFog Node management (OOB)

Network TSN, TCC, Comms, …	Accelerators FPGA, GPGPU, …	Compute	Storage

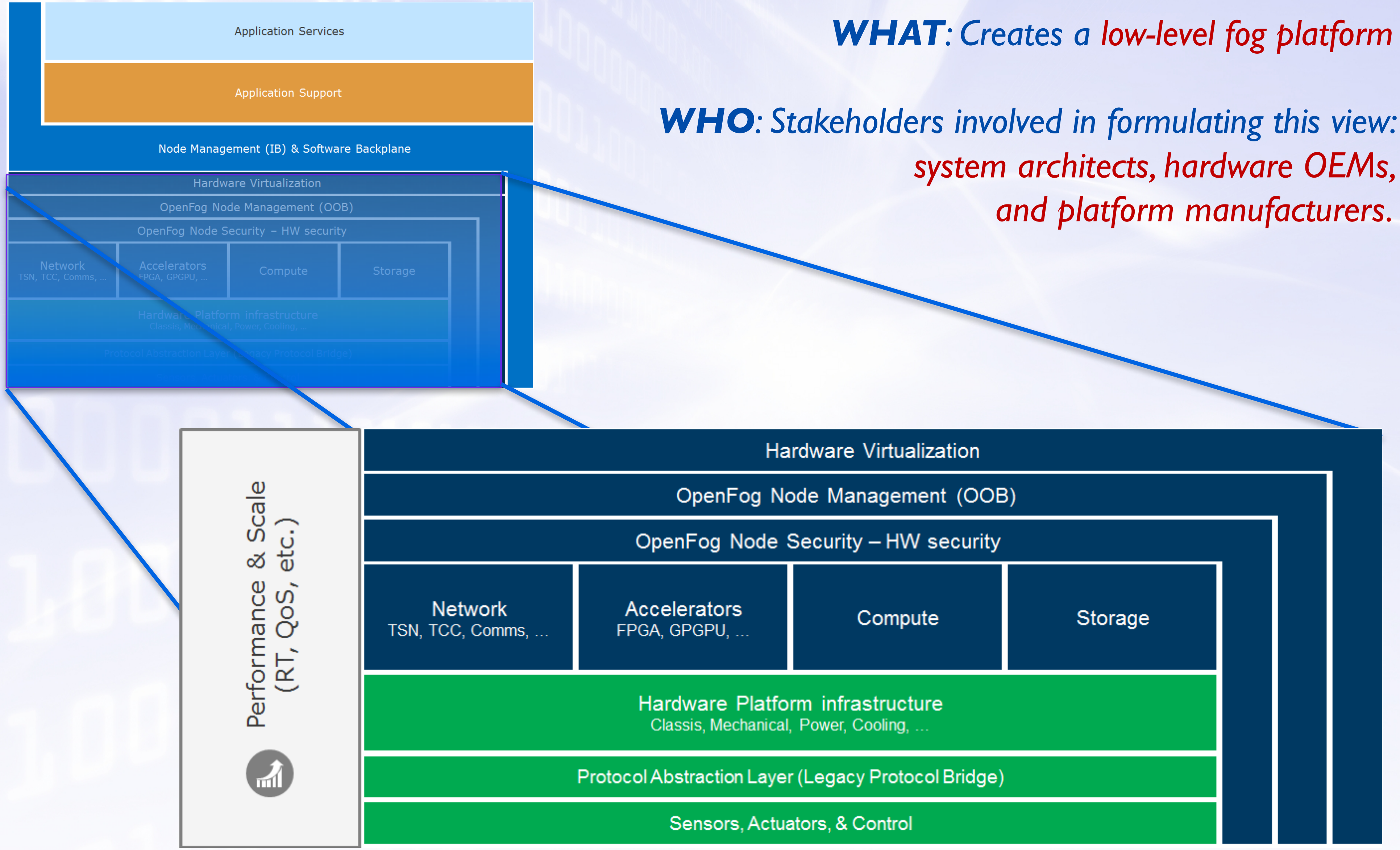
Protocol Abstraction Layer (Legacy Protocol Bridge)

Sensors, Actuators, & Control

OpenFog – View: System

***WHAT**: Creates a low-level fog platform*

***WHO**: Stakeholders involved in formulating this view: system architects, hardware OEMs, and platform manufacturers.*



Application Services

Application Support

Node Management (IB) & Software Backplane

Hardware Virtualization

OpenFog Node Management (OOB)

OpenFog Node Security – HW security

Network
TSN, TCC, Comms, …

Accelerators
FPGA, GPGPU, …

Compute

Storage

Hardware Platform infrastructure
Classis, Mechanical, Power, Cooling, …

Protocol Abstraction Layer (Legacy Protocol Bridge)

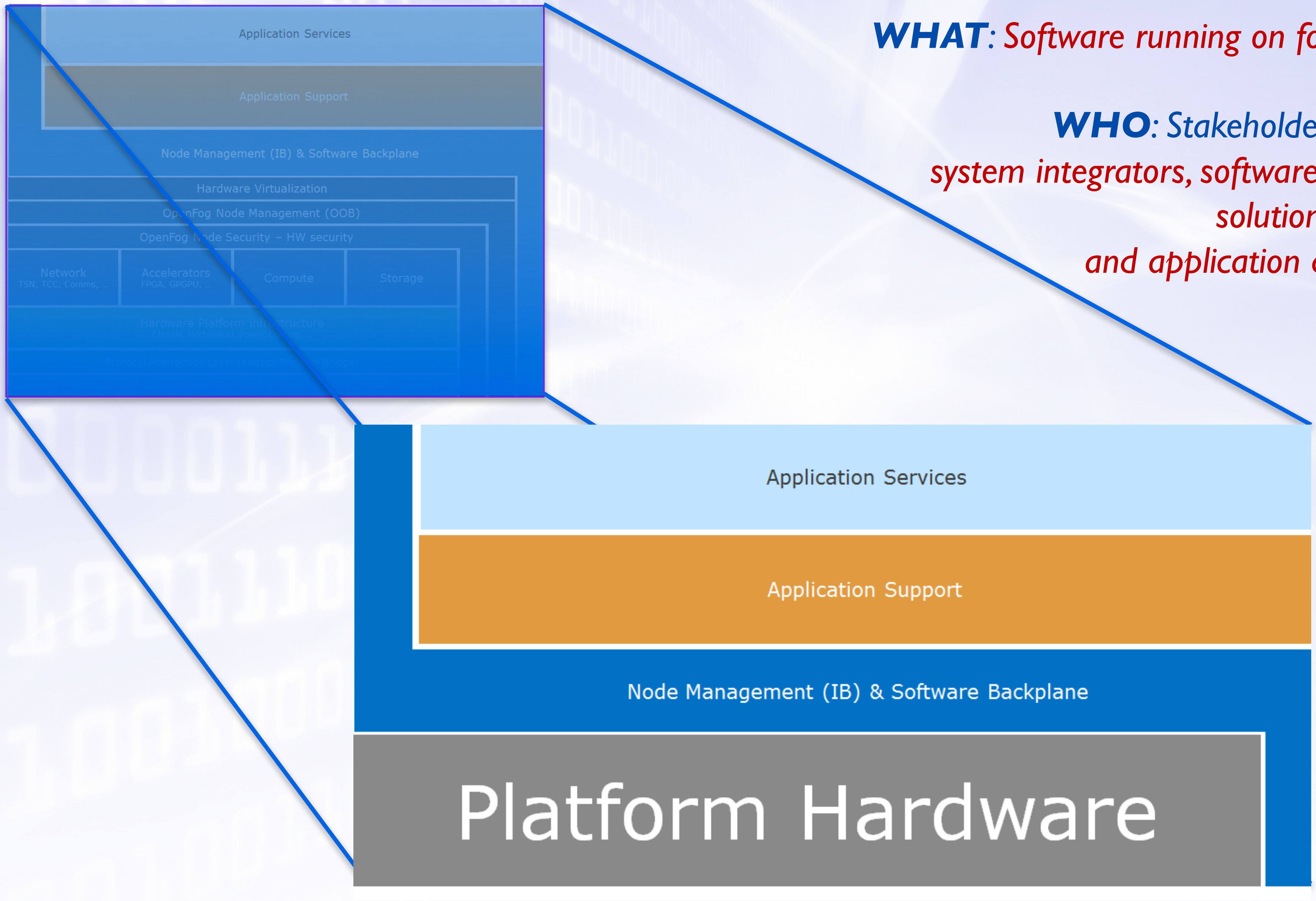
Sensors, Actuators, & Control

Performance & Scale
(RT, QoS, etc.)

OpenFog – View: Software

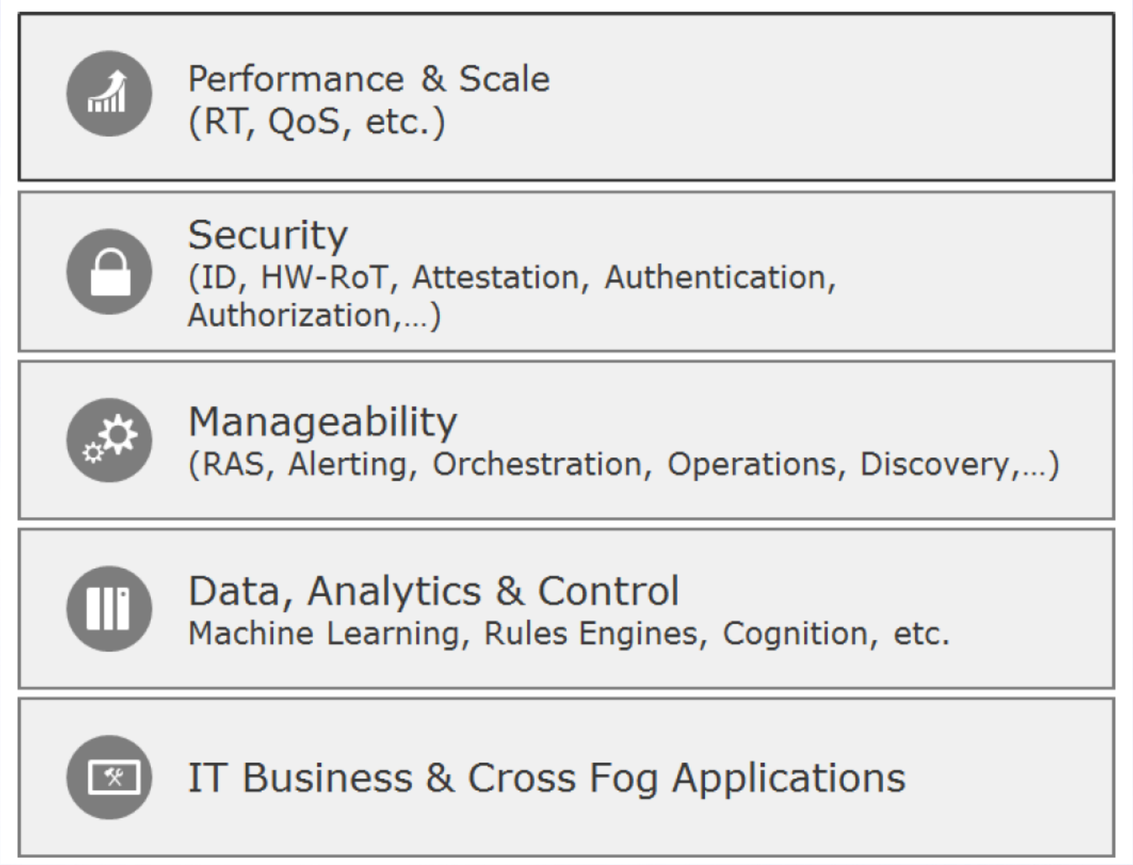
WHAT: *Software running on fog platform*

WHO: *Stakeholders involved:*
system integrators, software architects,
solution designers,
and application developers.


Application Services
Application Support
Node Management (IB) & Software Backplane
Hardware Virtualization
OpenFog Node Management (OOB)
OpenFog Node Security – HW security
Network
TSN, TCC, Comms, ...
Accelerators
FPGA, GPGPU, ...
Compute
Storage
Hardware Platform infrastructure
Chassis, Mechanical, Power, Cooling, ...
Protocol Abstraction Layer (Legacy Protocol Bridge)
Application Services
Application Support
Node Management (IB) & Software Backplane
Platform Hardware

OpenFog – Architecture: Perspectives

- Perspectives:
  - **Performance & Scale**
  - **Security**
  - **Manageability**
  - **Data, Analytics and Control**
  - **IT, Business and Cross Fog Apps**



Performance & Scale
(RT, QoS, etc.)

Security
(ID, HW-RoT, Attestation, Authentication, Authorization,…)

Manageability
(RAS, Alerting, Orchestration, Operations, Discovery,…)

Data, Analytics & Control
Machine Learning, Rules Engines, Cognition, etc.

IT Business & Cross Fog Applications

Multi-Access Edge Computing: Reference Architecture

European Telecommunications Standard Institute (ETSI)

FOSAD 2019

MEC Principles

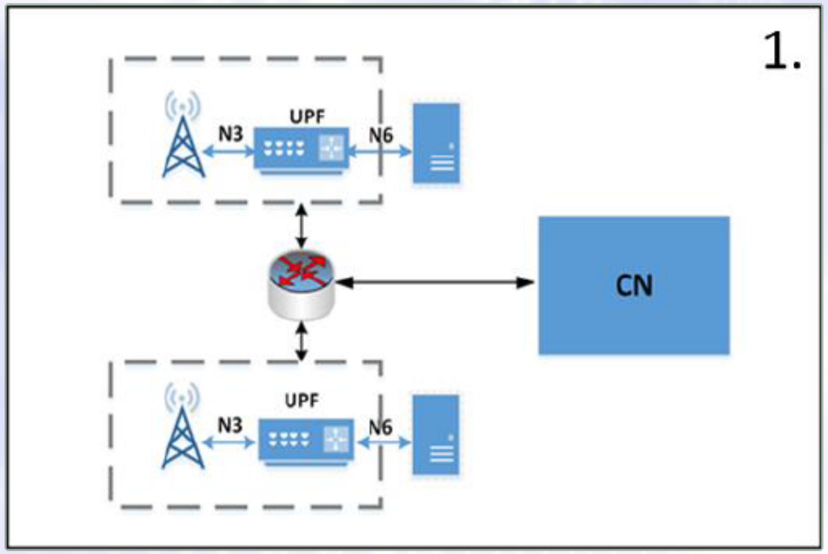
- Conceived to provide IT and cloud-computing capabilities within the RAN (Radio Access Network)
  - In other words: *Transform the 5G infrastructure into a cloud provider*

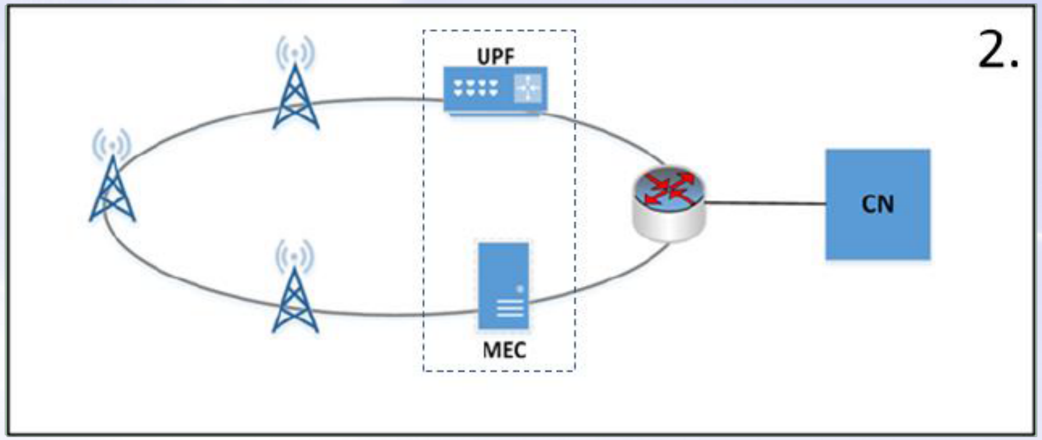
A. Mobility support: *"MEC systems need to support continuity of the service, mobility of application (VM), and mobility of user-related information (…) both to the edge and to the cloud."*

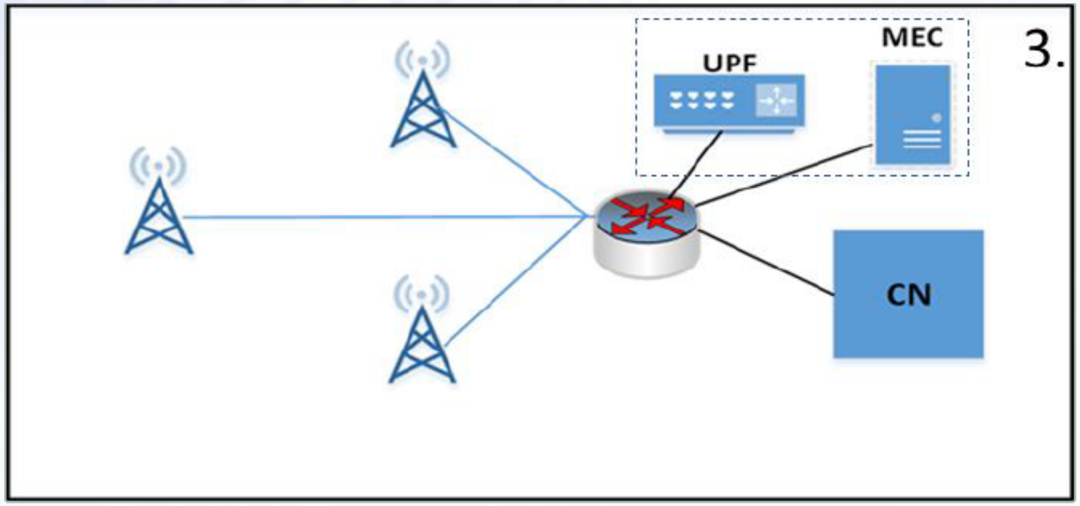
B. Deployment independence: *"Different deployment scenarios must be supported at the radio node, at an aggregation point, at the edge of the Core Network (e.g. distributed data centre) …"*

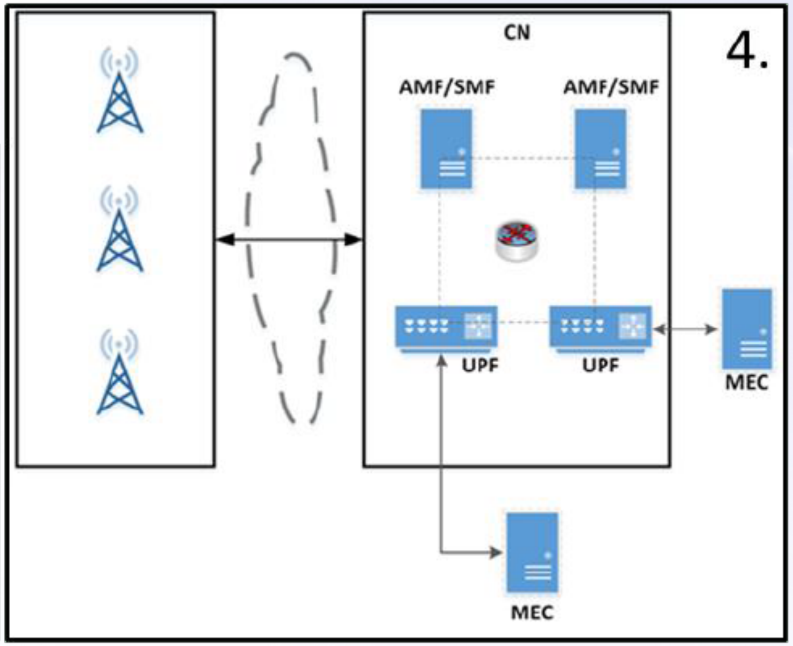
C. Smart Location: *"MEC applications need to run at the right place at the right moment, and might have to move when the conditions evolve."*

MEC Deployment



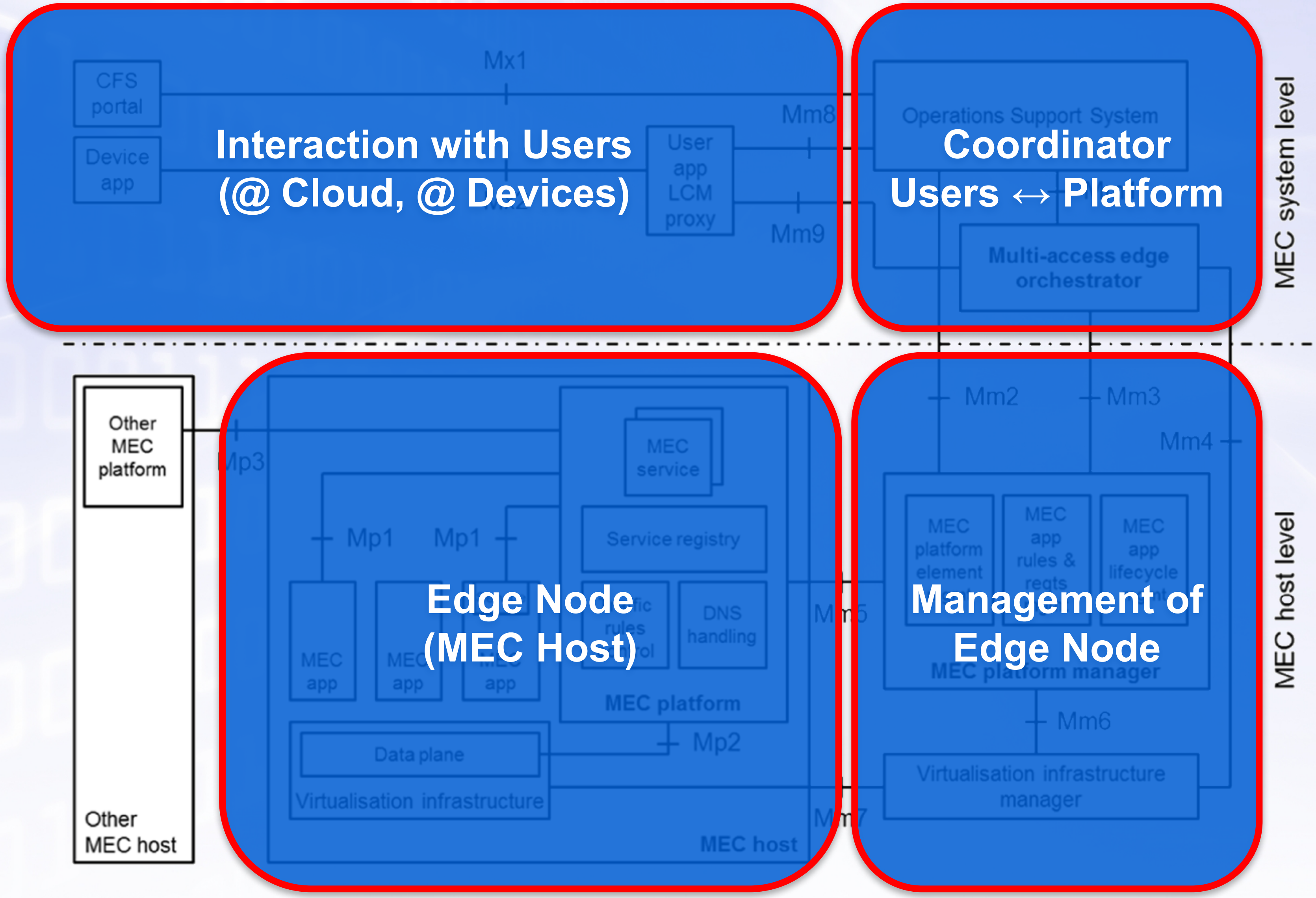






MEC – Reference Architecture (RA)

- Architecture: Collection of Components



Interaction with Users (@ Cloud, @ Devices)

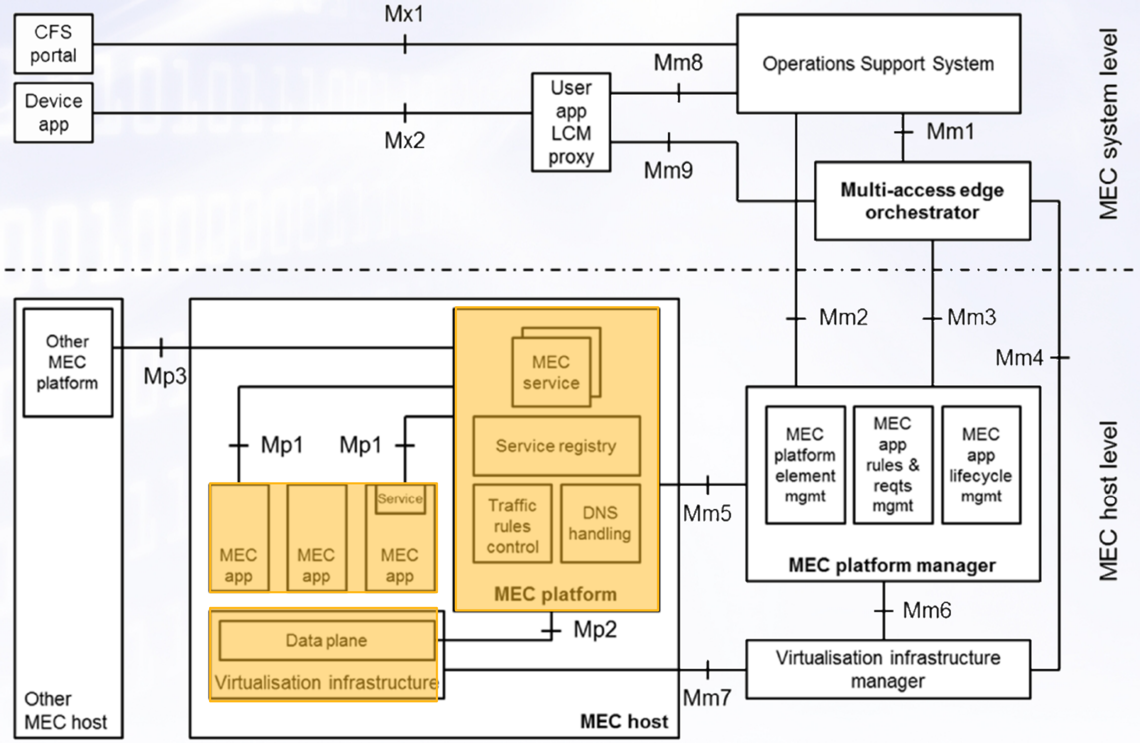
Coordinator Users ↔ Platform

Edge Node (MEC Host)

Management of Edge Node

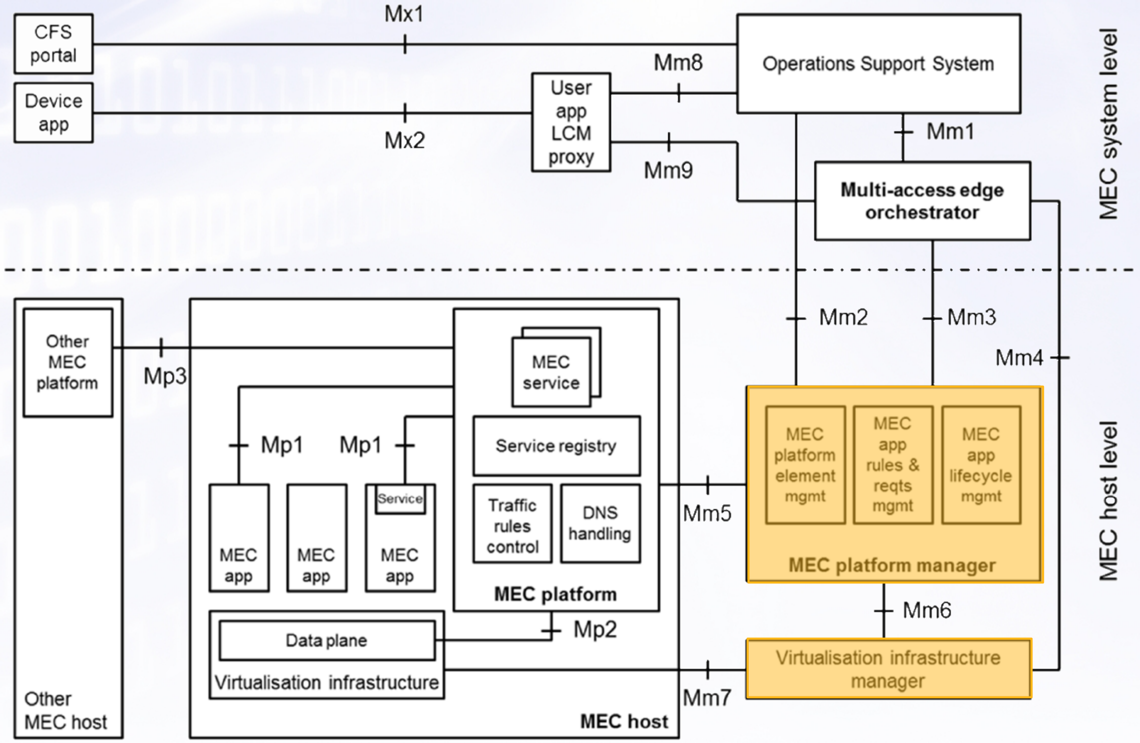
MEC – Reference Architecture (RA)

- MEC Host:
  - **MEC platform**
    - Provides the essential functionality required to i) *run MEC applications* and ii) *enable applications to provide and consume MEC services*.
  - **Virtualization infrastructure** which *execute MEC applications*
  - Also provides *storage and network resources*



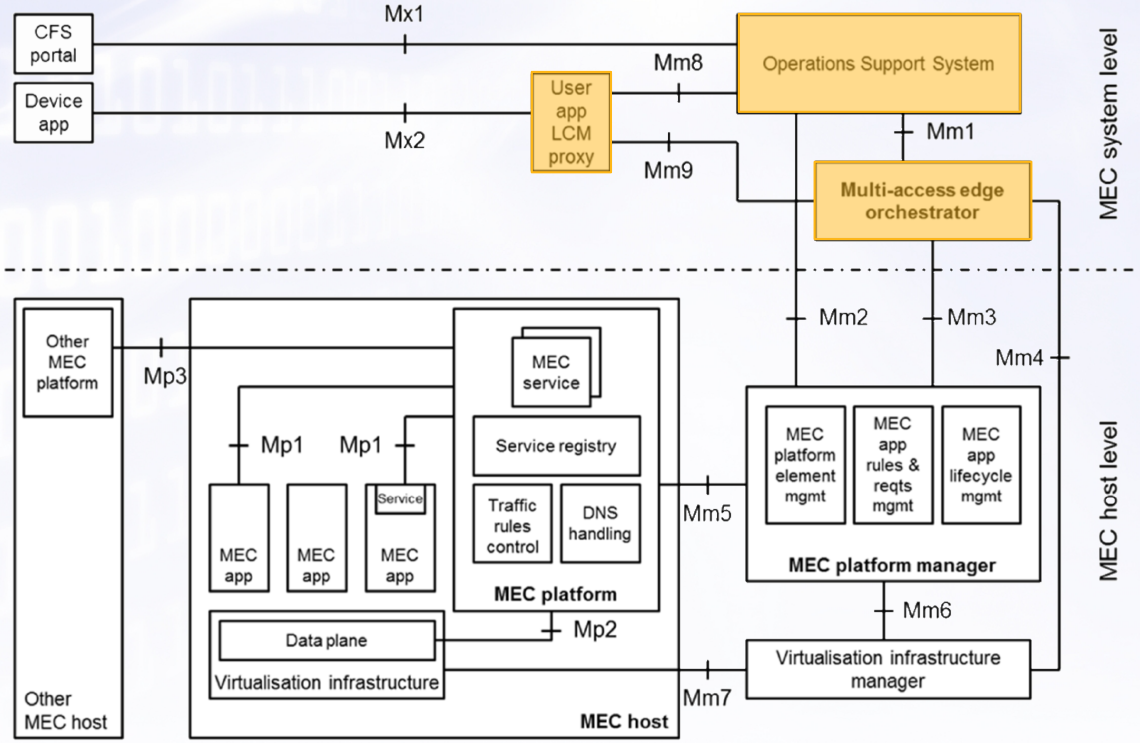
MEC – Reference Architecture (RA)

- Management of MEC Host:
  - **MEC platform manager**
    - *Manages a particular MEC host* and its applications' lifecycle
  - **VI manager**
    - *Prepares, allocates, manages, and relocates virtualized resources*



MEC – Reference Architecture (RA)

- System-level Management:
  - **Multi-access Edge orchestrator**
    - Core system level management component, *has an overview of the complete MEC system*
  - **User app LCM proxy**, **Operations Support System**
    - *Receives users (and devices) requests, checks authorization*



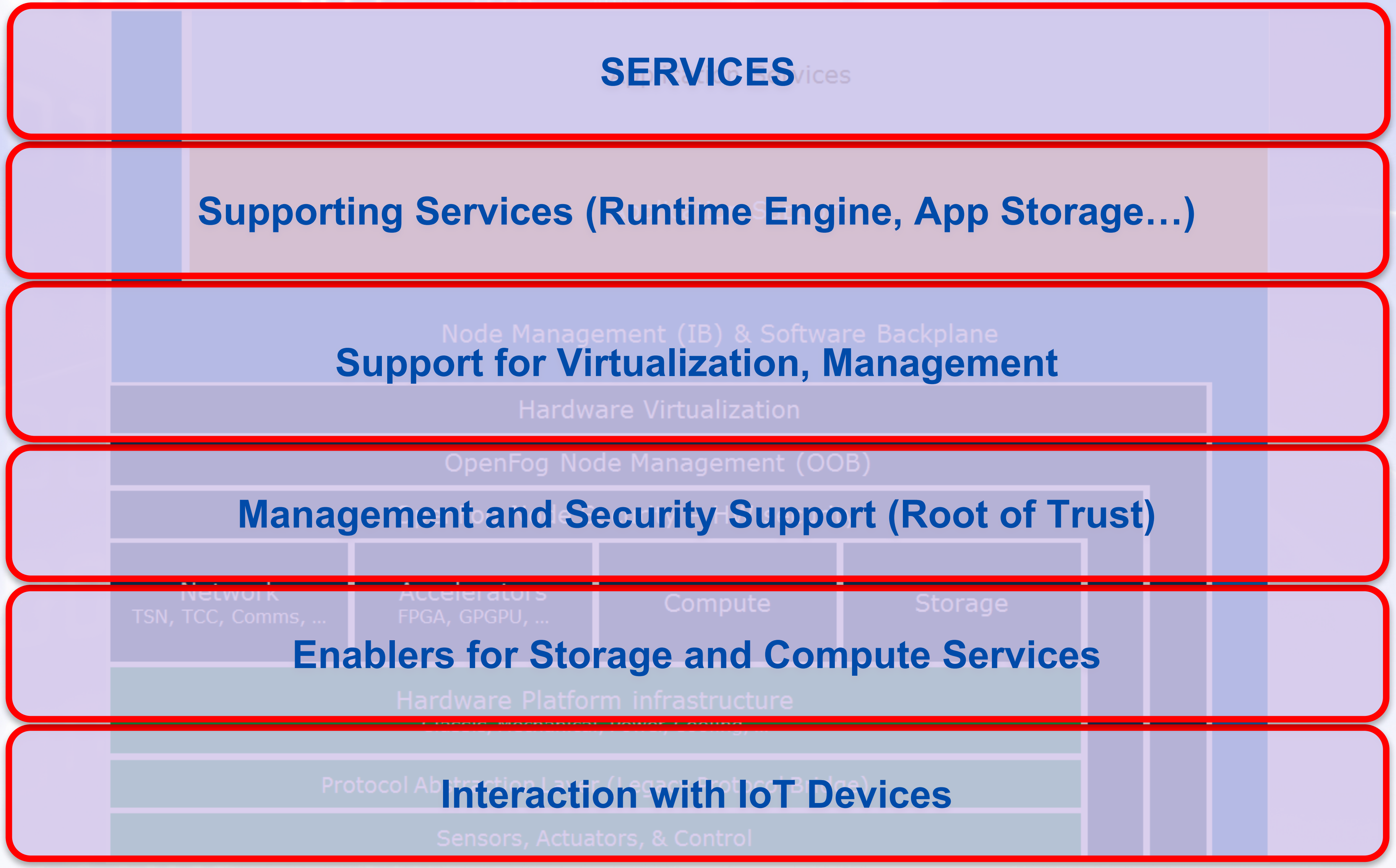
SECURITY IN OPENFOG AND MEC

OpenFog Reference Architecture (IEEE 1934-2018)

OpenFog Consortium –

Industrial Internet Consortium

OpenFog Reference Architecture



SERVICES

Supporting Services (Runtime Engine, App Storage…)

Support for Virtualization, Management

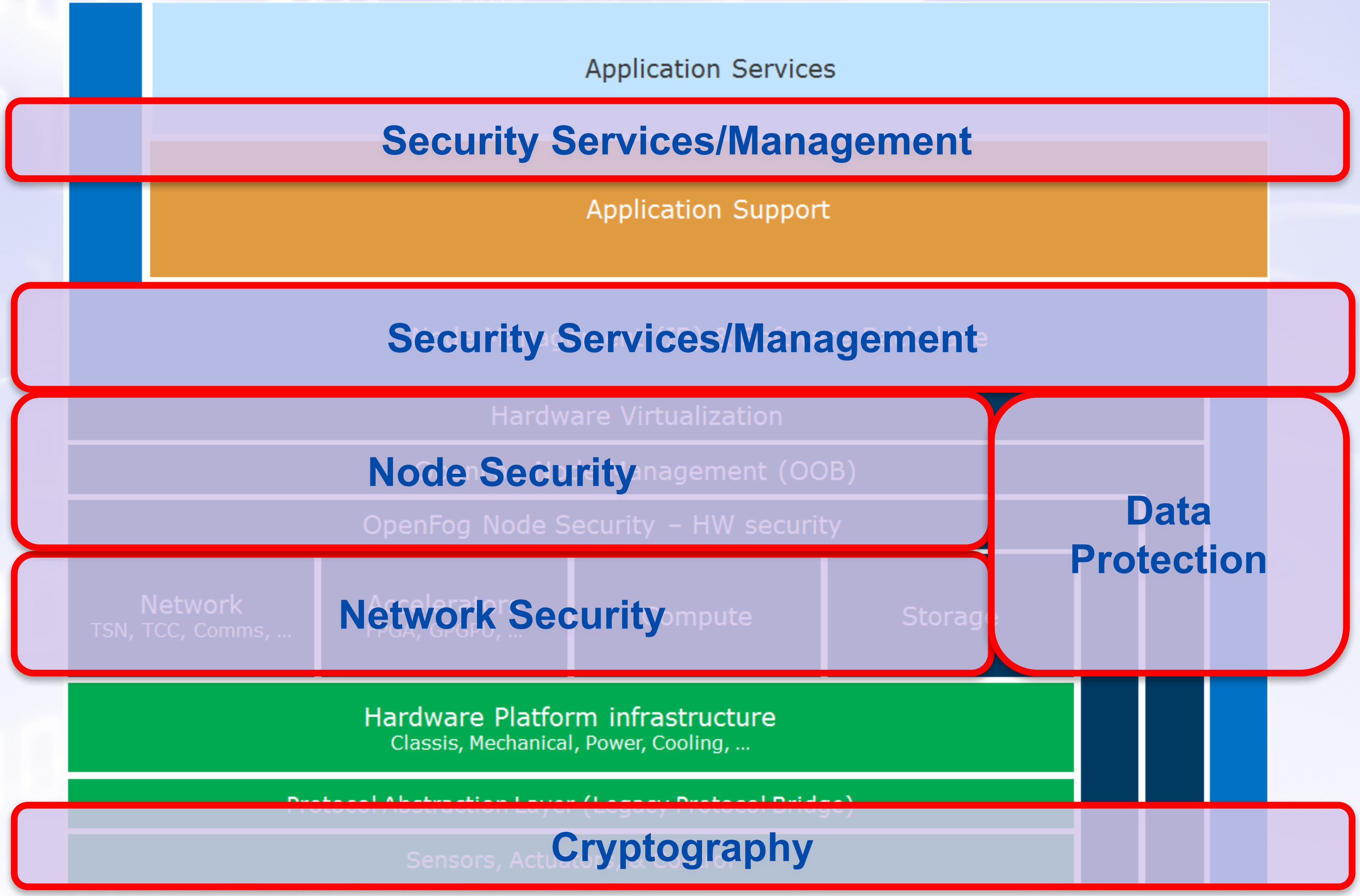
Management and Security Support (Root of Trust)

Enablers for Storage and Compute Services

Interaction with IoT Devices

vices
Node Management (IB) & Software Backplane
Hardware Virtualization
OpenFog Node Management (OOB)
Network
TSN, TCC, Comms, …
Accelerators
FPGA, GPGPU, …
Compute
Storage
Hardware Platform infrastructure
Protocol Abstraction Layer (Legacy Protocol Bridges)
Sensors, Actuators, & Control

OpenFog Reference Architecture - Security



Application Services

Security Services/Management

Application Support

Security Services/Management

Hardware Virtualization

Node Security

anagement (OOB)

OpenFog Node Security – HW security

Network
TSN, TCC, Comms, ...

Accelerators
FPGA, GPGPU, ...

Network Security

Compute

Storage

Data Protection

Hardware Platform infrastructure
Classis, Mechanical, Power, Cooling, ...

Protocol Abstraction Layer (Legacy Protocol Bridge)

Cryptography

Sensors, Actuators & Control

OpenFog Reference Architecture - Security

- Cryptography
  - Aim: Provide cryptographic mechanisms for the edge node
    - (A)Symmetric Key Ciphers, Cryptographic Hash Functions, Random Number Generators, Message Authentication Codes
  - This is provided by a 'Platform Security Processor' (PSP), if available
    - Provide support for virtual processors (vTPM)
    - May act as a secure vault for certificates, keys and passwords

- Network Security
  - Aim: Implement X.800 security services
    - Confidentiality, Integrity, Authentication, Authorization, …
  - Protocols included in the specification:
    - Node-to-Cloud/Node (WSS, (D)TLS)
    - Node-To-Device 802.1X, (D)TLS)
  - Services included in the specification:
    - Information flow analysis (DPI, IPS/IDS, lawful message interception)
    - Others (SDN/NFV)

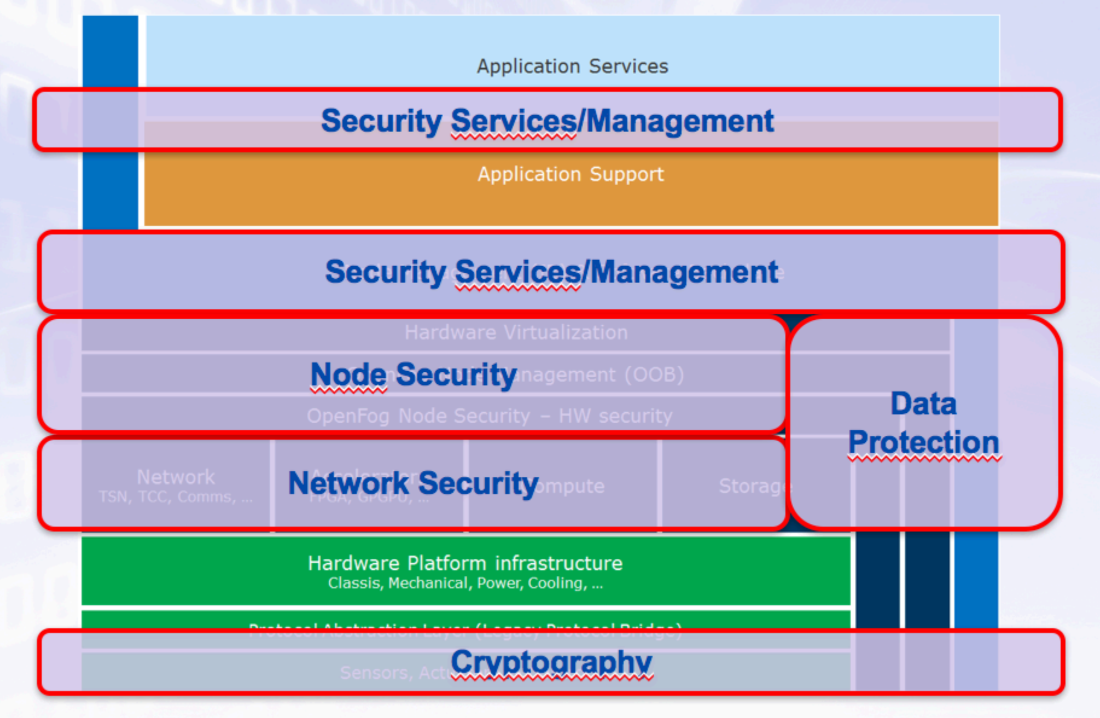
OpenFog Reference Architecture - Security

- Node Security
  - Aim: Protect both the node and the virtualization architecture
    - Based on Trusted Platform Modules (TPM), Trusted Execution Environment (TEE)

- Data Protection
  - Aim: Protect the information at all levels
  - Several strategies considered:
    a) "In use": Memory protection, trusted hypervisors
    b) "At rest": Encryption (at various levels), access control
    c) "In motion": Encryption (at infrastructure level, node level)

OpenFog Reference Architecture - Security

- Services
  - Aim: Provide supporting services (security and beyond)
  - *Software Backplane:* Virtualization support, Containerization support
  - *Application Support:* Entity registration, Proxy services, Secure Credential Storage
  - Under Consideration:
    - Concept of Decentralized Domains / Bridging entities
    - Security-as-a-Service, Blockchain/Smart Contracts, …

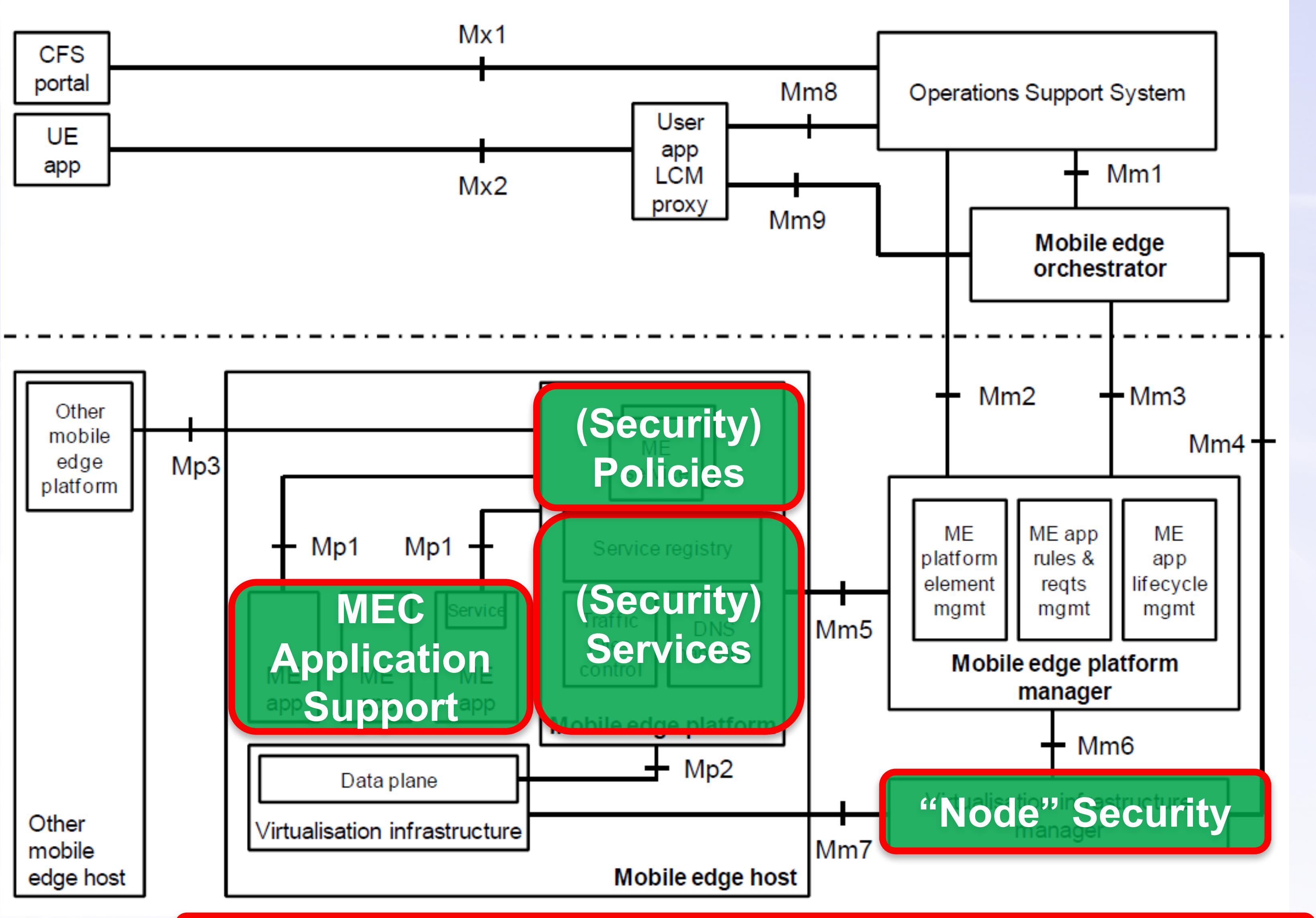

Application Services
Security Services/Management
Application Support
Security Services/Management
Hardware Virtualization
Node Security
nagement (OOB)
OpenFog Node Security – HW security
Network
TSN, TCC, Comms, ...
Network Security
FPGA, GPGPU, ...
ompute
Storag
Data Protection
Hardware Platform infrastructure
Classis, Mechanical, Power, Cooling, ...
Protocol Abstraction Layer (Legacy Protocol Bridge)
Cryptography
Sensors, Act

Multi-Access Edge Computing: Reference Architecture

European Telecommunications Standard Institute (ETSI)

FOSAD 2019

MEC Architecture - Security



Authentication / Access Control in (all) elements

MEC Architecture - Security

- **Authentication**
  - Aim: Authenticate all actors / components

  a) Request-response operations: REST + OAuth 2.0

  b) Certain topic-based message buses: DTLS + Certificates

- **Authorization / Access Control**
  - Aim: Services only accessed by authorized actors

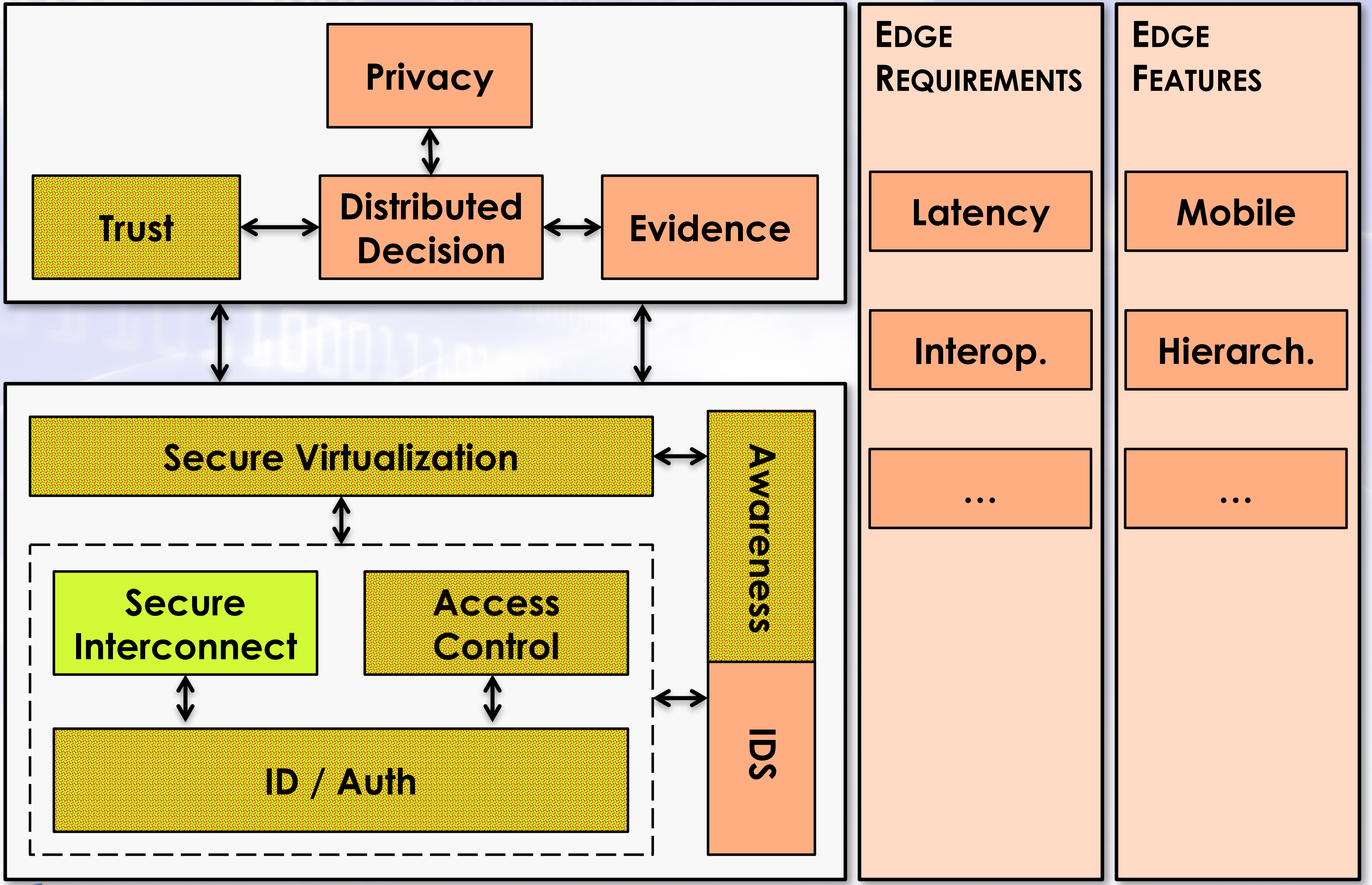
  a) Access Token
    - Permission Identifiers represented as OAuth 2.0 scope values
    - Others: Analyze the frequency of API calls.

  b) Certificates
    - Permissions (access to specific topic) mapped to client identifier (DN)

MEC Architecture - Security

- Mobile Edge Applications (VMs)
  - Aim: Ensure that all VMs can be trusted
  - Authenticity and Integrity: Digital signatures, Hashes
    - Package-level, file-level
    - Manifest includes {file list, provider certificate}
  - Policies: Check operator's policies + 3rd party service providers' requirements
- Mobile Edge Services
  - Aim: Services that support security and privacy operations
  - 👁 Location: 'Anonymous Customer References' mapped to resources/user(s)
- Platform
  - Aim: Secure VM lifecycle
  - This is linked to NFV specification, under development

Current Situation – Edge Standards



Security Mechanisms – Comparison

Security Service	OpenFog	Multi-Access Edge Computing
Secure Interconnection	**WSS, (D)TLS, VPN, IPsec**	**(D)TLS**
Identity, AuthN / AuthZ	Key Management, Security Policies	**(D)TLS, OAuth 2.0, Requirements and Constraints**
Secure Virtualization	**Root of Trust, Virtualization Architecture**	*(Linked to NFV specification)* **MEC Application**
Situation Awareness	DPI, IDS/IPS	-
Trust Services	**Attestation**	-
Distributed Decision	*(Under analysis)*	-
Privacy Support	Memory and disk encryption	User privacy
Evidence / Forensics	-	-

RESEARCH ON EDGE SECURITY

(BEYOND THE PREVIOUS ARCHITECTURES)

NICS

State of the Art – Major works

- **Authentication and Identity Management**
  - Even if mature, there are various open issues in the context of the Edge:
    - All the existing solutions depend on an online Third Party
    - Very few solutions consider the existence of a federated edge

i. User authentication towards Edge infrastructure

- Basic Authentication: a third party distributes secrets
  - Symmetric keys: Better performance with master secret key
  - Public keys: Improved security with certificates
- Attribute-Based Authentication: associate keys to attributes that need to be satisfied to enable decryption
  - Policy based: use CP-ABE to enable authenticated communications with fog nodes and the cloud

ii. Edge supporting user authentication

- Biometric Authentication: biometric information is either processed or encrypted in edge devices

State of the Art – Major works

- **Privacy Mechanisms**

i. Identity Privacy

- Anonymous Authentication: enable anonymous authentication of users and devices with the edge
  - Pseudonyms, Ring signatures, IBC, Blockchain
  - Some works suggest the use of Tor anonymity network to protect the identities of users and services

ii. Context Privacy:

- Private task allocation: Optimally assign services to users without revealing their exact location to the server in the cloud
  - User location obfuscation at the edge

State of the Art – Major works

- **Privacy Mechanisms**

iii. Data Privacy:

- Data at rest: has mostly focused on access control although some work has also been done on searchable encryption
  - Attribute-based encryption, proxy re-encryption, Shibboleth, distributed hash tables, …
- Data processing: most works have dealt with computations over encrypted data and secure data aggregation
  - Homomorphic encryption, multiparty computation, secret sharing, differential privacy, …

iv. Privacy Support

- Privacy agent: Trusted agent that enforces data privacy policies
  - Secure data bundling, behaviour monitoring

State of the Art – Major works

- **Anomaly and Intrusion Detection Systems**
  - Detection: How to detect anomalies
    - Specific detection mechanisms are necessary due to intrinsic features of the edge infrastructure (VMs, SDN y NFV), what affects to detection strategies of external and internal attackers
    - Detection granularity. Every tier (device, Fog, Cloud) has access to different information, what affects the detection mechanisms
  - Deployment: How to distribute the agents
    - Securing one or two tiers of the network architecture is not sufficient to protect the entire system (three tiers)
      - dangerous events like the propagation of malware from a compromised device to the rest of the network could not be noticed
    - The Fog could be very complex and geographically worldwide distributed, depending on the purpose for which it was designed
      - an IDS should be able to provide a real-time protection to the entire architecture.

State of the Art – Major works

- **Anomaly and Intrusion Detection Systems**
  - Reaction:
    - If IDS solution includes different modules, they still need to cooperate, adding further typical distributed systems' challenges.
    - Early discover of intrusion violation is difficult because:

      (i) huge number of connected edge devices,

      (ii) geographic distances (impact on the network latency)

      so complicating analysis of packets in real-time.

      It is a challenge to decrease notification time, to minimize impact on the response time.

State of the Art – Major works

- **Trust Management**
  - *Major open issues:*
    - Cloud and Edge nodes are assumed to be trustworthy, or their trustworthiness is evaluated with the same mechanism
    - Again, very few solutions consider the existence of a federated edge

i. Trust-based resource allocation: which Edge node more suitable to host certain resources given our requirements

- Considered so far: (i) the current performance (traffic flows and tasks), (ii) the previous experience and context, (iii) the existence of transitive trust paths

ii. Trust between infrastructure elements:

- Interaction with IDS: edge nodes collect data and perform data analysis for detecting malicious nodes

State of the Art – Major works

- **Digital Evidence**
  - Specific main challenges:
    - How to acquire *data* from entities connected to the Edge system
    - How to spread *Data* across the Edge-Cloud continuum
    - How to build chain of custody (integrity, origin, and trustworthiness of *data*)

i. Retrieving data from (IoT) devices at the Edge
   - Register interactions between (IoT) devices
     - Network traffic, location, flow of data

ii. Proactive Forensics
   - Using SDN to redirect suspicious traffic for future forensic analysis
   - Using NFV to "freeze" suspicious VMs and store for future forensic analysis

State of the Art – Major works

- **Virtualization – SDN & NFV**
  - Can be extremely useful in the context of edge paradigms for:
    - isolating unsecure devices (and traffic under adversarial conditions)
    - directing the traffic towards security devices
    - reconfiguring the systems in real time

➢ *Security challenges in SDN*

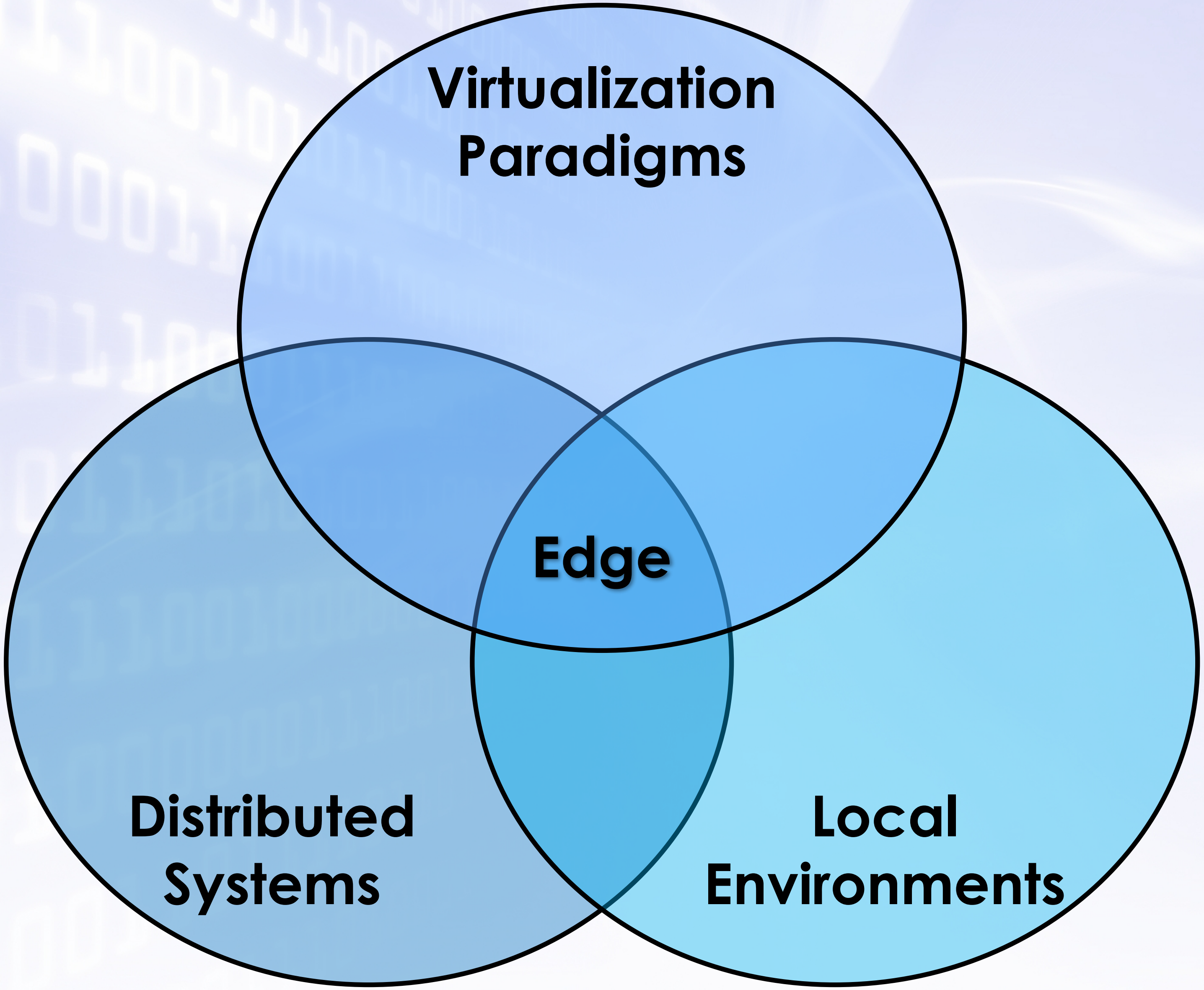
- Little exploration on distributed control planes (focus on centralization)
  - Single point of failure, fragile implementations, scalability issues…
- Improve security capabilities
  - Better security APIs, better monitoring tools, better policies…

➢ *Security challenges in NFV*

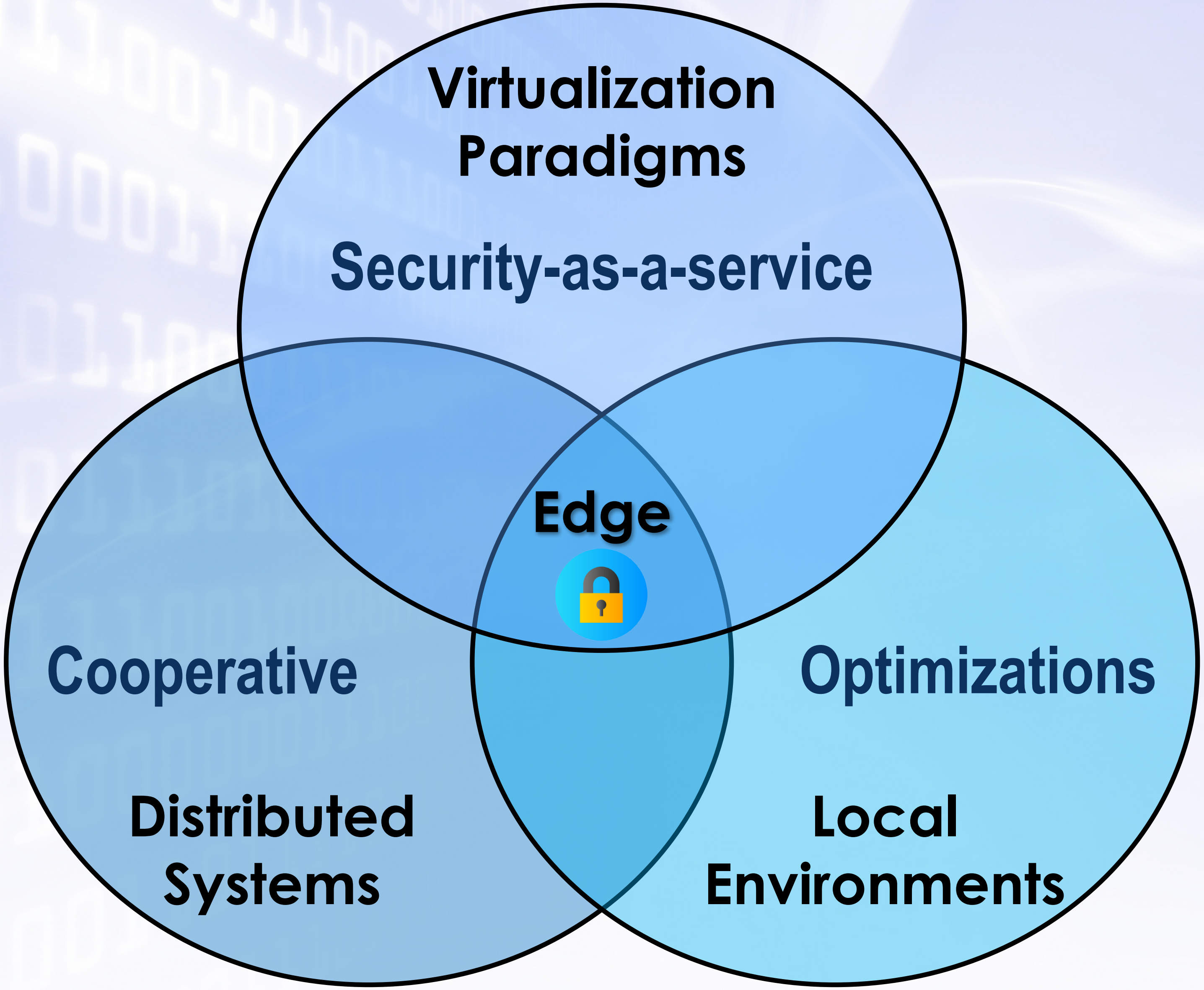
- Traditional virtualization challenges
  - Side-channel, flooding, hijacking, injection attacks…
- Challenges specific to existing NFV standards
  - Security management and orchestration, configuration complexity…

EDGE COMPUTING AS A SECURITY ENABLER

Why "Security Enabler"?



Why "Security Enabler"?



Virtualization Paradigms

Security-as-a-service

Edge

Cooperative

Distributed Systems

Optimizations

Local Environments

Virtualization and Sec-aaS

- Main technologies:
  - **NFV**:Virtualization of computational resources
  - **SDN**: Flexible and dynamic networks managed by software
- **Reminder**: Cloud computing core features
  - *On-demand self-service* → Sec. services deployed where needed
  - *Broad network access* → Security services are easily accessible
  - *Resource pooling* → Interaction with edges and clouds
  - *Rapid elasticity* → Facilitates scalability of security services
- Corollary: Security services can be deployed any*
  - Anytime, anywhere, anyhow
  - Not only computational services, but other resources can be managed in a dynamic way!
    - Network connections

Distributed Systems and Cooperation

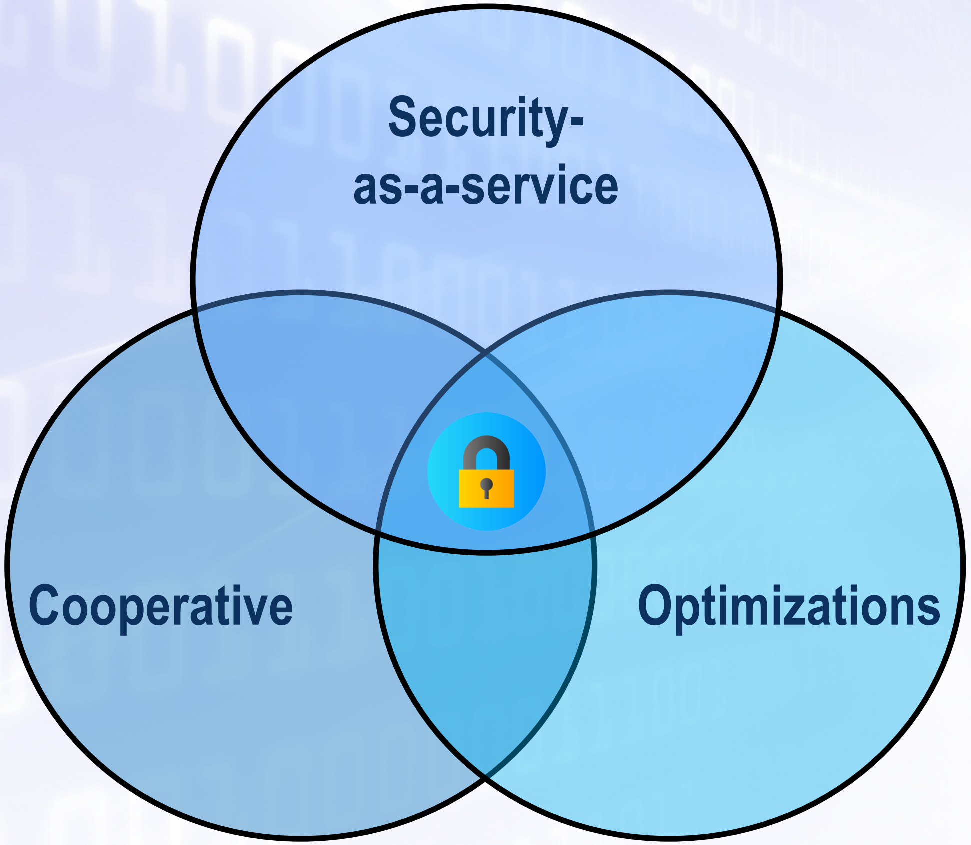
- Ecosystem:
  - Multiple Cloud providers
  - Multiple (potential) Edge Computing layers
  - Multiple Users

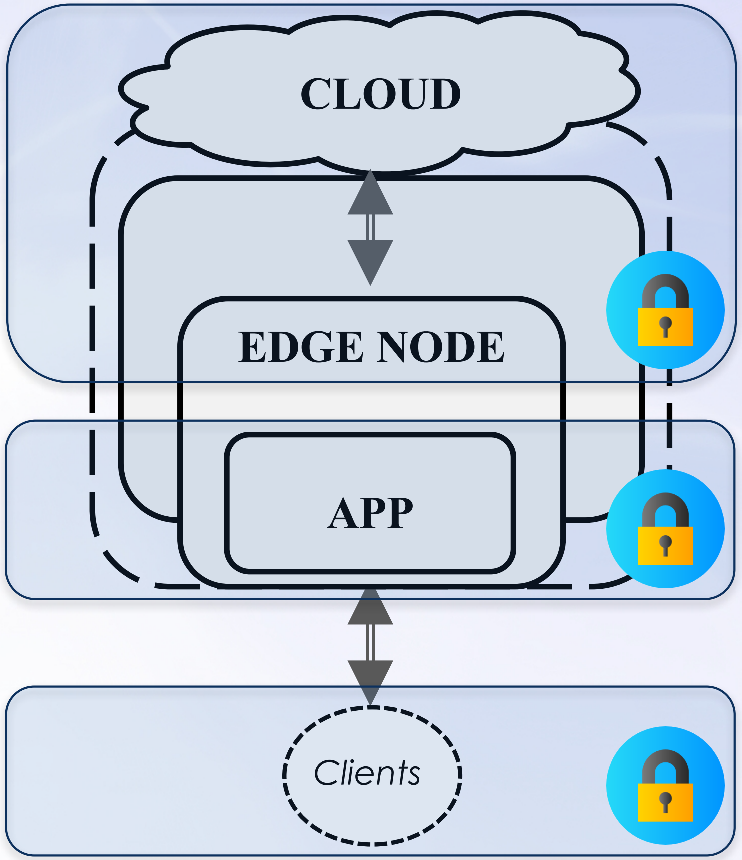
- Therefore, multiple opportunities for cooperation, vertically and horizontally
  - *Delegation of tasks*
    - e.g. Execute resource-consuming tasks, process local information
  - *Distribution of tasks*
    - e.g. Analyze a spike of potentially malicious traffic, deploy tasks in specific layers / locations
  - *Duplication of tasks*
    - e.g. "Digital twins" in Industry 4.0

Local Environments and Optimizations

- **Reminder**: Edge computing core benefits
  - *Low latency and jitter*
  - *Reduced overall network bandwidth*
  - *Context awareness*
  - *Mobility support*
- Services deployed @ Edge enjoy such benefits
  - ➢ (Security) services can be optimized!
  - Quick access to security services
    - Not only for users, but for services and infrastructure as well
  - Security services manage local information
    - E.g. Important in services such as Intrusion Detection
  - Certain security services can "follow" the user
    - "*Follow*": either the machine / container, or its state
    - E.g. security helpers such as proxies, privacy assistants…

Why "Security Enabler"?





- Helpful not only for protecting the edge infrastructure itself, but for protecting the apps/services deployed in the edge, and even the clients.

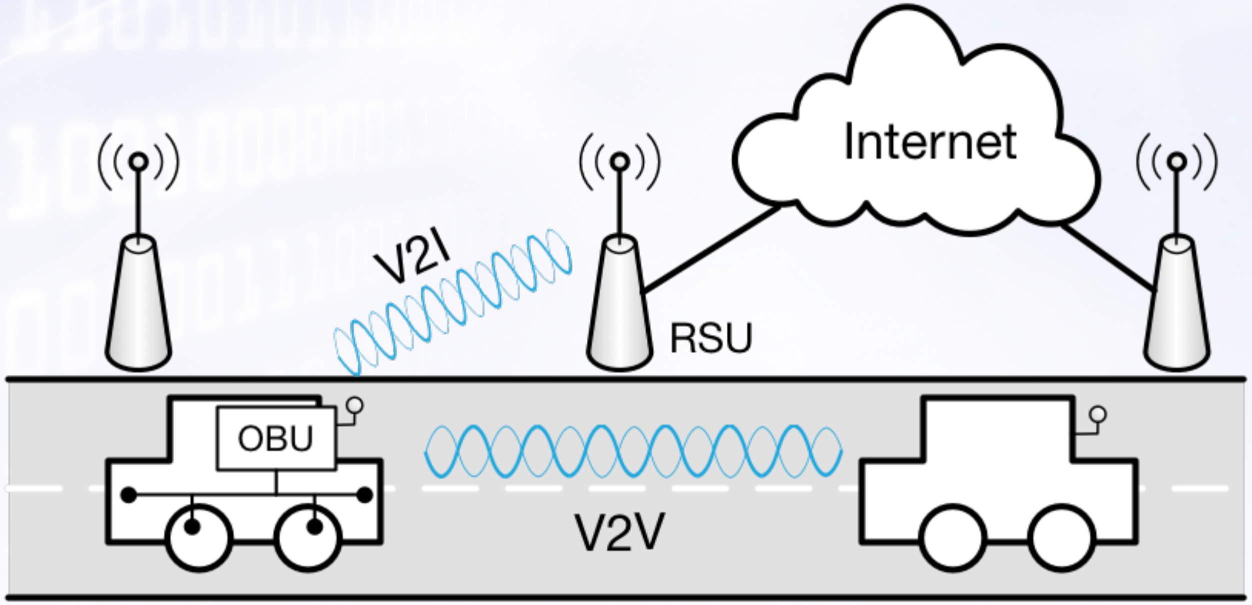
EXAMPLES OF USING THE EDGE FOR ENHANCED SECURITY

SECURITY IN EDGE-POWERED VEHICULAR NETWORKS

Context: Vehicular Network

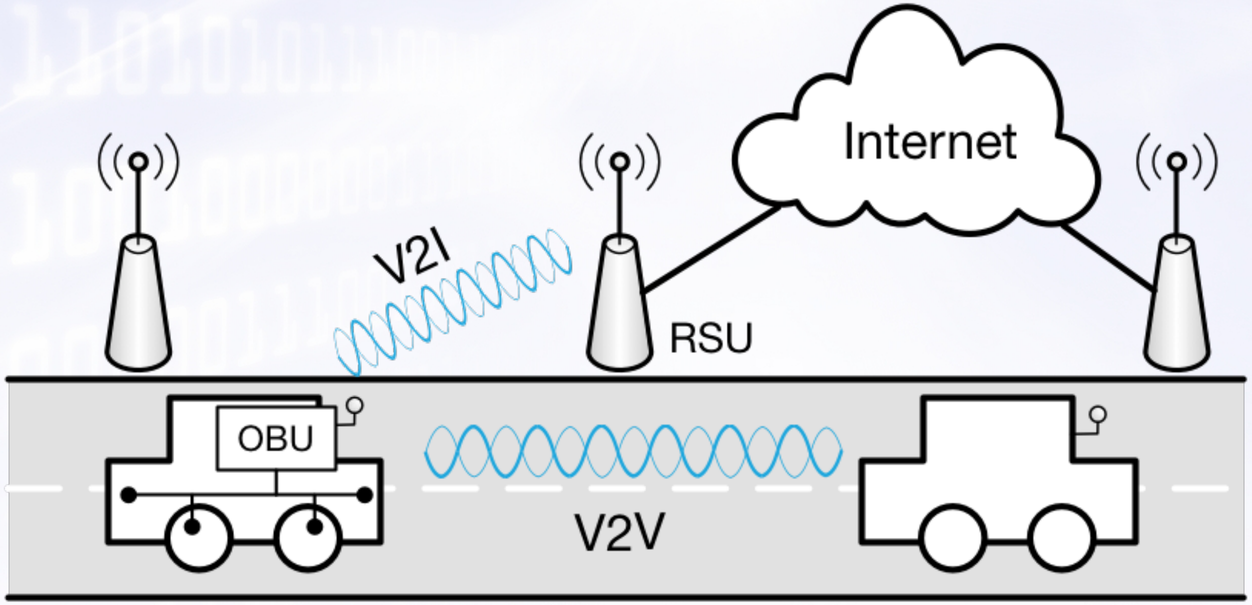
- Vehicular Networks can be seen as the core element of Intelligent Transportation Systems
  - posing a number of unique challenges

- Vehicles equipped with sensing technologies
  - communicating with each other (V2V)
  - and with the roadside infrastructure (V2I)



Context: Vehicular Network

- Vehicle nodes have limited but sufficient computing and storage capabilities thanks to on-board units (OBU)
- The static nodes of the network are road-side units (RSU)
- V2I comm. rely on cellular technologies (e.g. LTE)
- V2V comm. rely on dedicated protocols (e.g. DSRC/WAVE)



Vehicular Networks: Security Challenges

- **Authentication**
  - Extremely important to avoid fake/malicious messages
  - Existing solutions and standards typically rely on PKI to solve authentication problems
  - Extensively researched issue, with various known phases:
    - ITS initialization: All entities (RSUs, OBUs) register with the ITS authority and obtain valid credentials
    - Communication: V2I and V2V messages are sent using the credentials obtained previously
    - Verification: Vehicles need to verify the integrity and authenticity of credentials
    - Revocation: Invalid credentials should be revoked
  - **CHALLENGE**: The workload of managing revocation information mostly falls on the vehicles

Vehicular Networks: Security Challenges

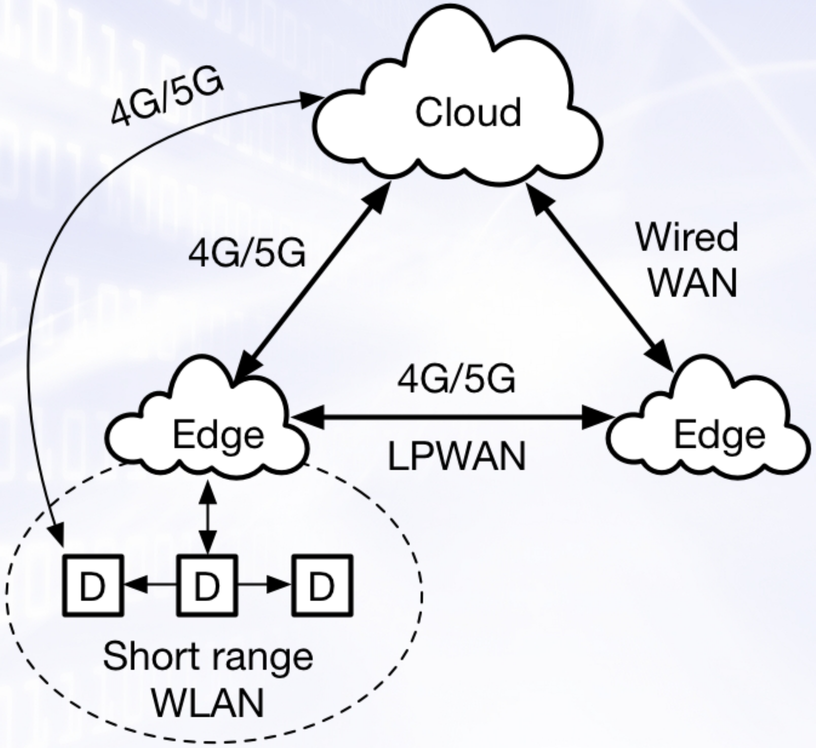
- **Anonymity**
  - Achieving authentication and privacy poses unique challenges
  - The most studied approach is the use of pseudonyms
    - Certificates are not directly linked to a real identity
    - Pseudonyms are issued either by a third party (e.g. ITS) or by the entity itself (e.g. OBU)
      - Trusted authorities should revoke user anonymity in case he misbehaves (e.g. use of escrow information)
    - To avoid traceability, pseudonyms need to change over time, location or context
      - (e.g. pseudonyms pools, changing on-demand)
  - **CHALLENGE**: Pseudonym update frequency can be very high. Also, the cost of pseudonym change is not negligible

Vehicular Networks: Security Challenges

- **Availability**
  - RSU might not be available at all times in all roads
  - V2V communications improves the efficiency of road traffic
    - Yet there might be disruptions due to high mobility of vehicles
  - **CHALLENGE**: The availability of existing Vehicular Networks must be improved

- **Digital Evidence**
  - Little research on this subject
  - Only partial solutions exist with *a* limited scope:
    - Evidence generation – without analysis of secure storage
    - Evidence witnessing – only from the point of view of the vehicles
  - **CHALLENGE**: *Advances* in this research area are needed

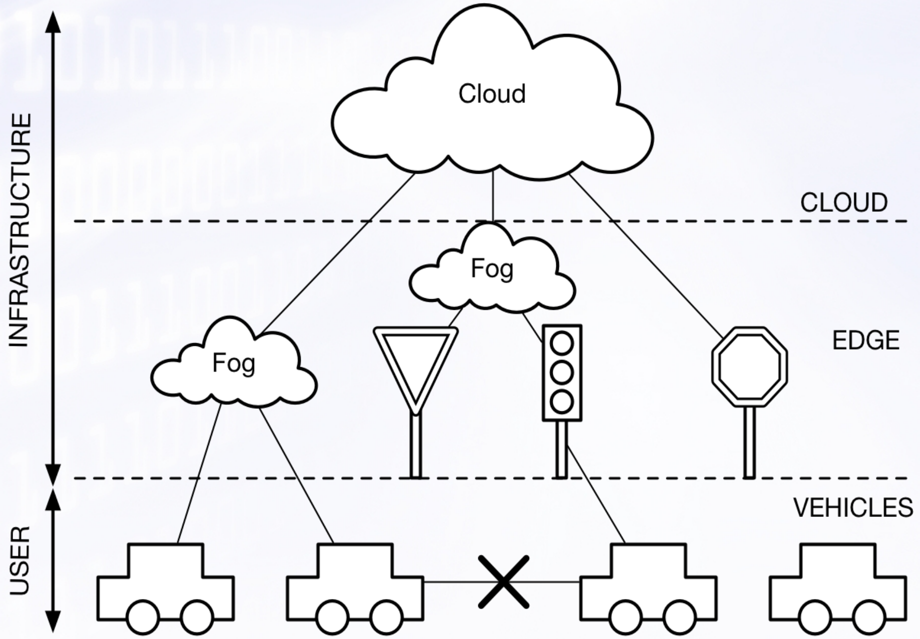
Edge-Assisted Security



Let’s add some Edge to the mix…

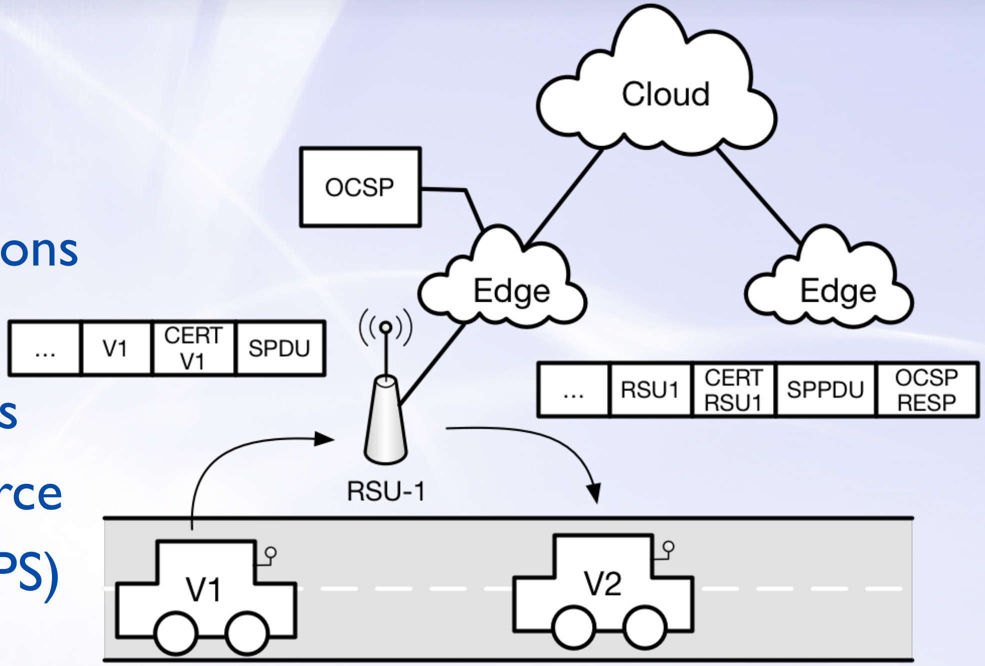
VN + Edge = Vehicular Edge Computing

- Three approaches:
  1) *Fog-based*: General-purpose fog/edge devices assist vehicular networks
  2) *RSU-based*: Enhanced RSU units provision security services
  3) *Hybrid Fog/RSU*: Dedicated and general-purpose edge devices coexist and are (typically) organized in two tiers



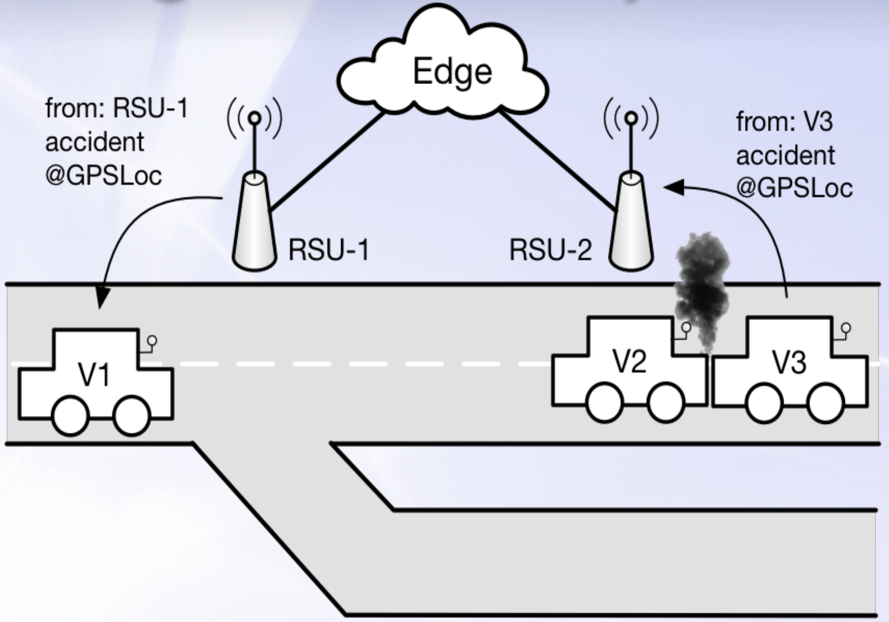
Vehicular Edge Computing and Security

- **Authentication**
  - Beacon and safety messages are only sent using V2I communications



  - Messages received by edge nodes are modified to include new source and required information (e.g. GPS)
  - Edge nodes verify revocation status of the vehicle that transmits the message
    - Vehicles only need to verify revocation status of edge nodes
  - **BENEFIT**: CRL management is simplified
    - CRL management can be distributed, and update intervals can be reduced
    - Other techniques (*Delta CRLs, OCSP*) can also be used

Vehicular Edge Computing and Security



- **Anonymity**
  - Sending data through an edge device can hide the original data sender
    - Transformation of the messages hide the original sender from remote vehicles
  - **BENEFIT 1**: Less pseudonym changes are needed, as less entities are aware of the pseudonym of a vehicle
  - Additional identity privacy: As data goes up, data can be (geo)aggregated
    - and context-aware services be provided to wider - and less accurate - geo positions
  - **BENEFIT 2**: Upper layers will not contain identifying information

Vehicular Edge Computing and Security

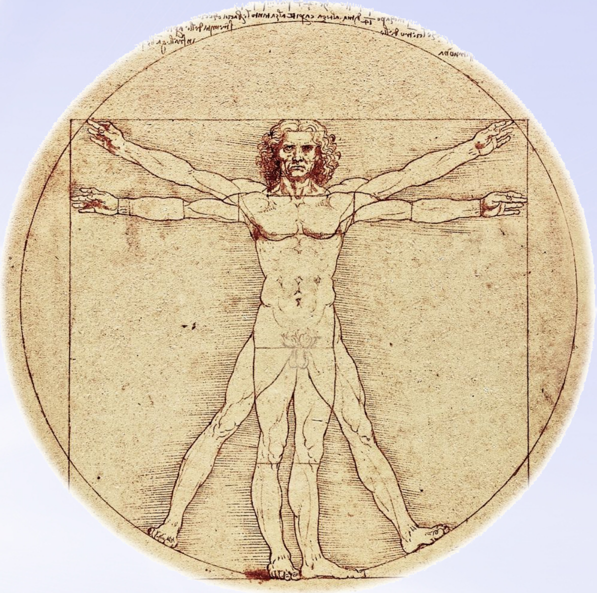
- **Availability**
  - Edge deployments are likely to be based on the 5G infrastructure
    - Coverage provided by the 5G cellular network
    - Intermediate edge nodes will have more protection against HW attacks (e.g. root of trust, anti-tampering mechanisms)
  - No over-deployment: services can be scaled according to need
  - **BENEFIT**: Improved availability and flexibility in resource usage

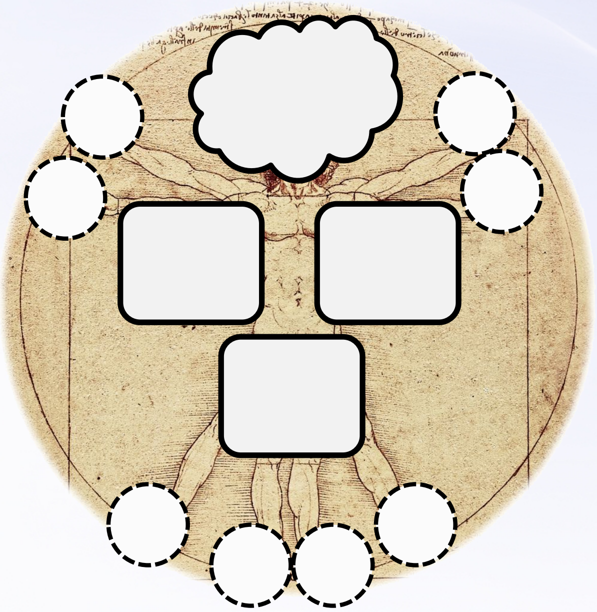
- **Digital Evidence**
  - Edge nodes can keep evidence of received messages
  - Evidence can be relayed upwards and analyzed for misbehavior
    - The higher the level, the more powerful the analysis can be
  - **BENEFIT**: Evidence can now be analyzed and stored

ADVANCED SEC. SERVICES @ EDGE: "IMMUNE SYSTEMS"

Why an "immune" system?

- Many immune system-inspired mechanisms already exist:
  - From specific detection mechanisms to various learning strategies
- Yet: The Edge/IoT has various similarities with the human body
  - Multitude of "cells" distributed in a certain area
    - With the possibility to include a central brain that supervises everything
  - "Cells" (and pathogens!) can move from one place to the other
  - "Cells" can perceive and interact with the environment and other "cells"





Why an "immune" system?

- GOAL: Create a system that *fulfils the same requirements as the Human Immune System*
  - **Flexibility**: Immune cells should specialize in different functions
    - E.g. Macrophages: body sentinels; Neutrophils: killer cells
  - **Mobility**: Immune cells should move within our body
    - E.g. From our bone marrow to the infected areas of our body
  - **Lightweight**: Immune cells should be small and quick
    - E.g. Immune cells have a similar size to other mobile cells
  - **On-Demand**: Immune cells should appear when needed
    - E.g. The immune system produces more cells when we are sick
  - **Adaptability**: Immune cells should adapt to new illnesses
    - E.g. New antibodies are generated for new illnesses
  - **Protection**: The immune system should not attack the host
    - E.g. Immune cells can recognize what is part of our bodies
    - We have to lessen the risk of "autoimmune diseases"!

Elements of an immune system

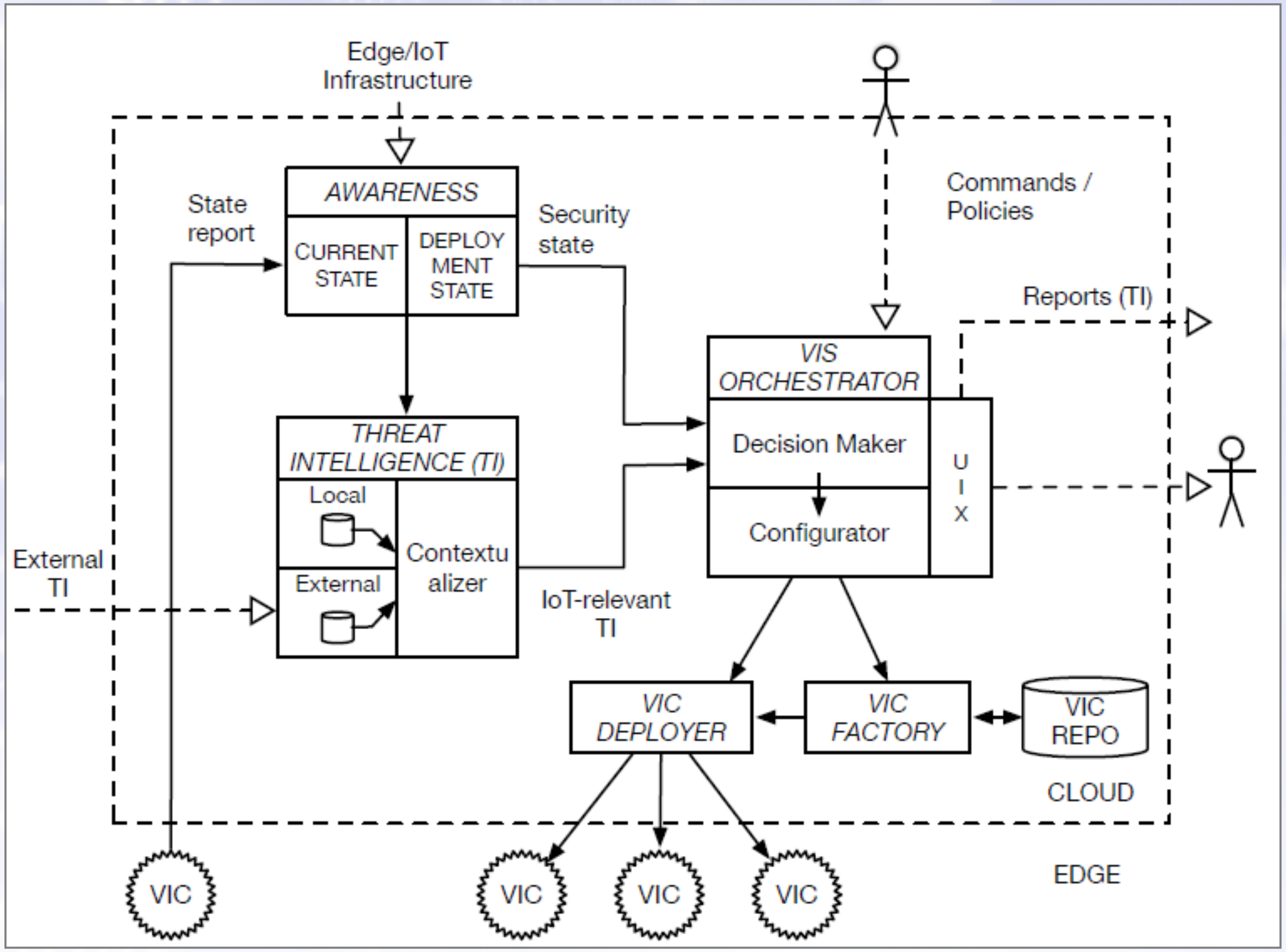
Virtual Immune Cell (VIC)

- Deployed *at the Edge*
- *Virtual appliance* (from VM to lightweight containers)
- Equipped with a *base code* (common to all cells) and with *specific modules*
- Can *interact with all entities* (Edge node, cloud, monitored system)

Virtual Orchestrator

- Located *in the cloud*
- Receives *inputs* from internal and external systems
- Makes *decisions on the configuration and deployment* of the VICs
- Provides various *outputs* and reports for human actors and other systems

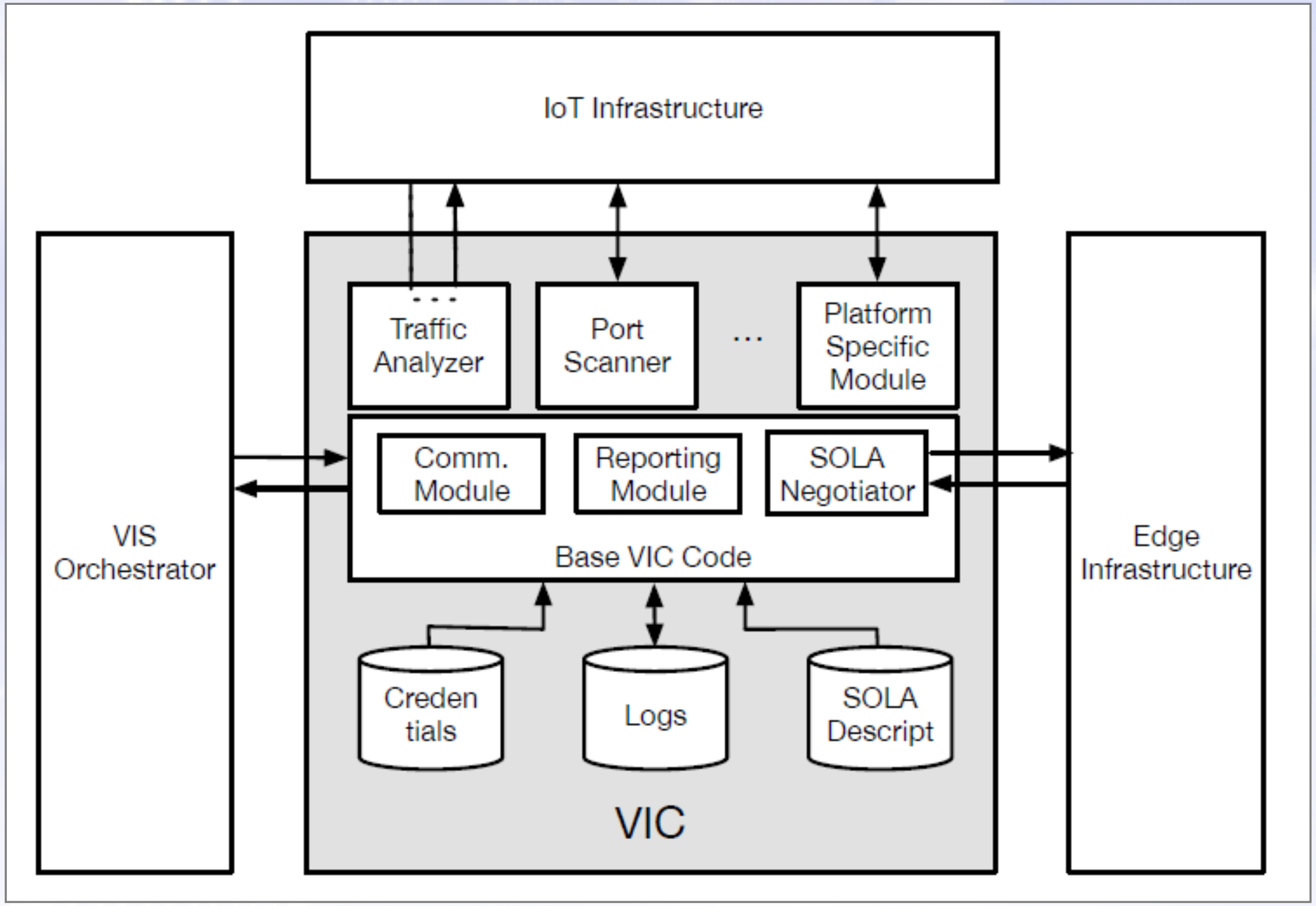
Virtual Orchestrator



VICs are prepared to manage specific issues (**Flexibility**, **Adaptability**)

VICs are deployed when and where needed (**On-Demand**)

Virtual Cell



VICs – Virtual specialized appliances (**Lightweight**, **Mobility**)

VICs can negotiate their tasks with the Edge Infrastructure (**Protection**)

Deployment of the Immune system

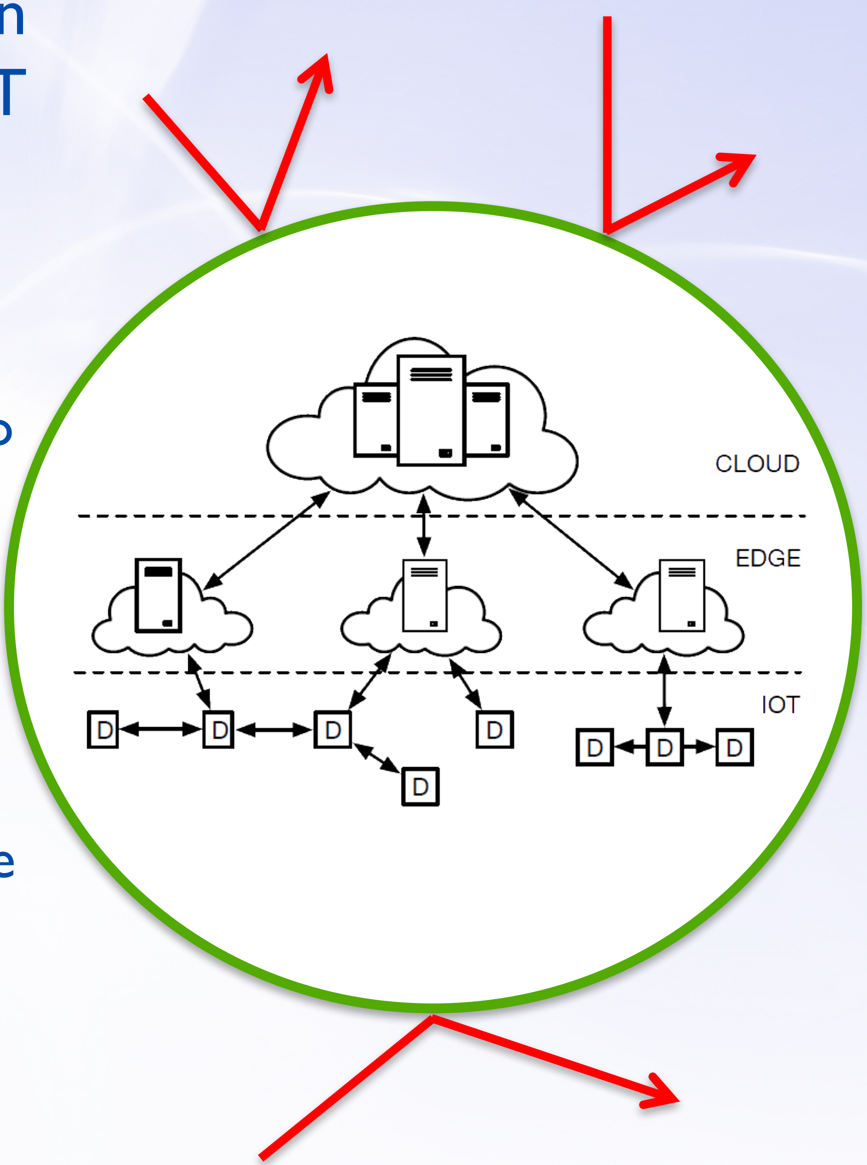
- Most Edge standards are still a work in progress…
- …yet they seem to support our requirements
  - Availability of a *virtualization infrastructure*
  - Existence of *deploying mechanisms* for the virtual immune cells
    - MEC: Interactions with the Operations Support System
    - Fog: Northbound interfaces
  - *Connectivity* with the monitored systems
    - MEC: Components that interconnect virtual machines in a network
- Other aspects must be further explored
  - Security Operations Level Agreement, SOLA
    - Aims to solve the "Who watches the Watchmen" conundrum
    - Virtual Immune Cells must provide information regarding what they are going to test, where, when, and how
    - Any deviation should cause the termination of the cell

Deployment of the Immune system

- What about the implementation of the cells?
  - *Virtual Appliance*: Multiple strategies (full-fledged virtual machines, containers, more lightweight solutions) could be used
  - *Service Flexibility*: It is possible to use two strategies:
    - Mutation:Virtual Cells integrate a startup script that, after the first execution, downloads the software they need
    - Specialization:Virtual Cells are specifically created with the tools they need
  - *Geolocation*:Various mechanisms that allow the deployment of virtual machines depending on their location are being researched
  - *Integration*: In order to facilitate the interaction with the monitored system, the Orchestrator provides the necessary information (including temporary credentials) to the cells
  - *Functionality*: IoT-specific IDS, vulnerability testing, configuration testing, pentesting, fuzzying mechanisms, behaviour modelling…

Applicability

- It is obvious that this system can be used to protect Edge IoT deployments…
- …yet it can go beyond that!
  - *Virtual Immune Systems in other scenarios* (from distributed content to vehicular networks)
  - *Virtual Immune system for the Edge*: Protect the Edge infrastructure itself!
  - *Accountability and Service Assurance*: Virtual cells can implement any service (e.g. query capabilities of Edge nodes)



The Edge and the Immune System

- Immune System as an Advanced Security Service. Why?

A. It facilitates the protection of all actors

   i. *(Edge) Infrastructure:* The immune system can analyze the health of the Edge infrastructure itself

   ii. *Service Providers:* The services and components of service providers can be monitored by the immune system

   iii. *Users:* The interactions between the users and their services are also monitored by the immune system

   – …It is possible to instantly react against threats!

B. It takes advantage of all Edge features

   – *Security-as-a-Service:* Various testing, detection and analysis mechanisms can be deployed any*

   – *Cooperation:* Multiple subsystems can cooperate to create an adaptable protection layer

   – *Optimization:* Local information and warning can be provided "on site"

CONCLUSIONS

Edge Computing has its own security issues that need to be solved…

…yet it also enables the potential of various Edge-assisted security services

We should keep both points of view in our research!

Javier Lopez

Network, Information and Computer Security (NICS) Lab

University of Malaga

NICS