UNIVERSIDAD DE MURCIA

IoT in the Era of the Continuum Computing: Challenges and Opportunities

Antonio Skarmeta

Universidad de Murcia (Spain)

skarmeta@um.es

UNICO I+D

CERBERUS 5G

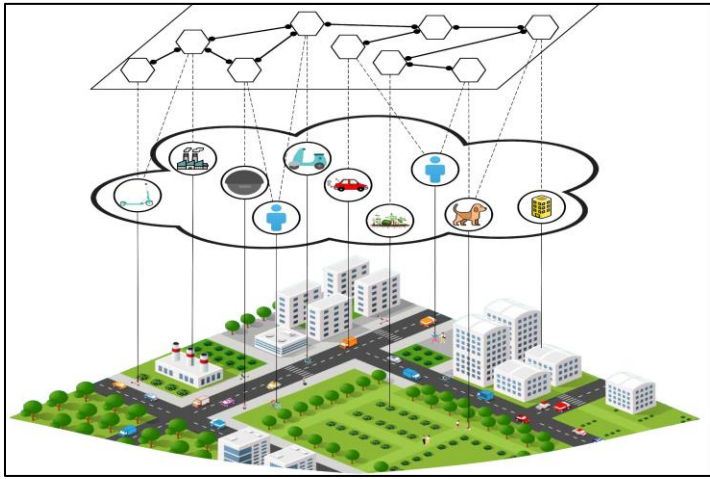
FLUIDOS

RIGOUROUS

R3CAV

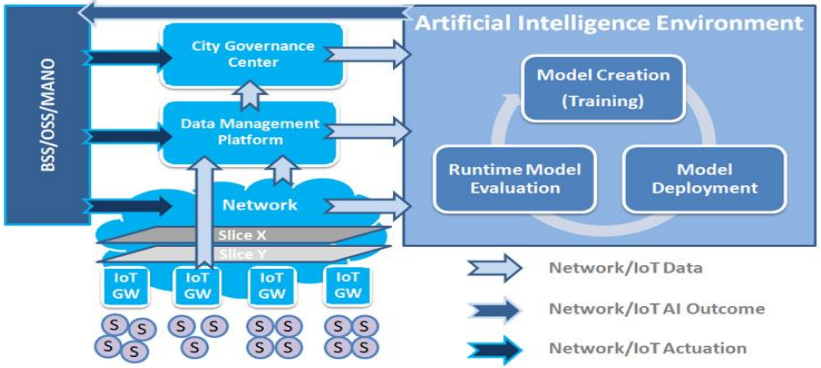
Opportunity

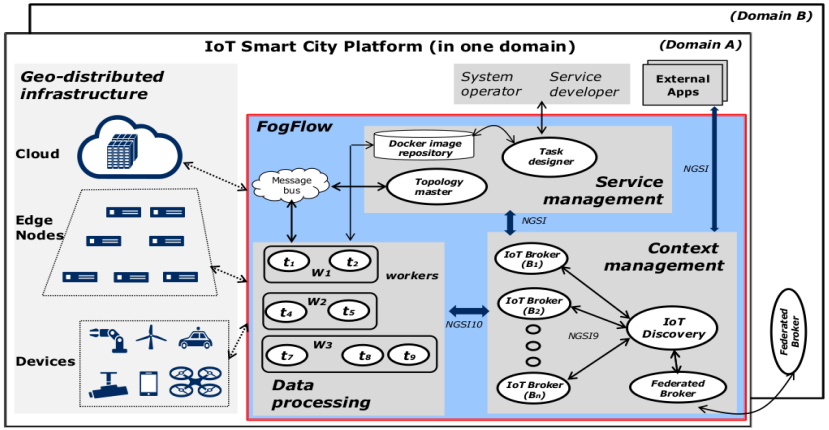
- IoT devices and the emergence of 5G in our daily lives are bringing new data-driven and increasingly autonomous scenarios.
- Possibilities of highly distributed processing capacties from IoT-Edge-Cloud in a continuum:
  - New services requires efficient and effective management of computing and network resources
  - Means to deal with huge amounts of data and at different levels of the future NG infrastructure

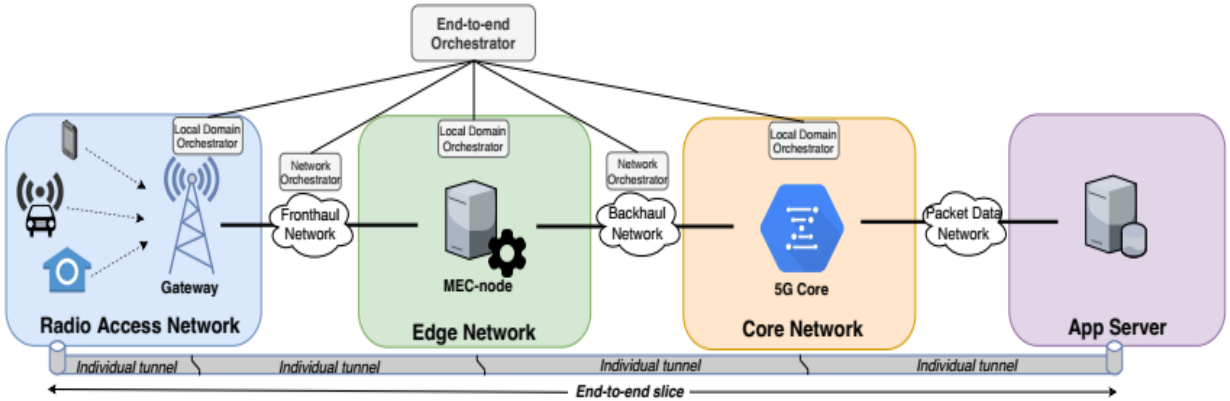


- Need for configuration, architecture and coordination of processing nodes at different levels: end-device – edge – cloud … and beyond
- Need for intelligent methods to offload processing operations to the proper levels of the computing network to meet e.g. delay and processing constraints
- Support heterogeneous processing infrastructures, offering decentralized and adaptive coordination of virtual resources that accommodate QoE, mobility and security requirements

IoT, 5G, Virtualization and Intelligent



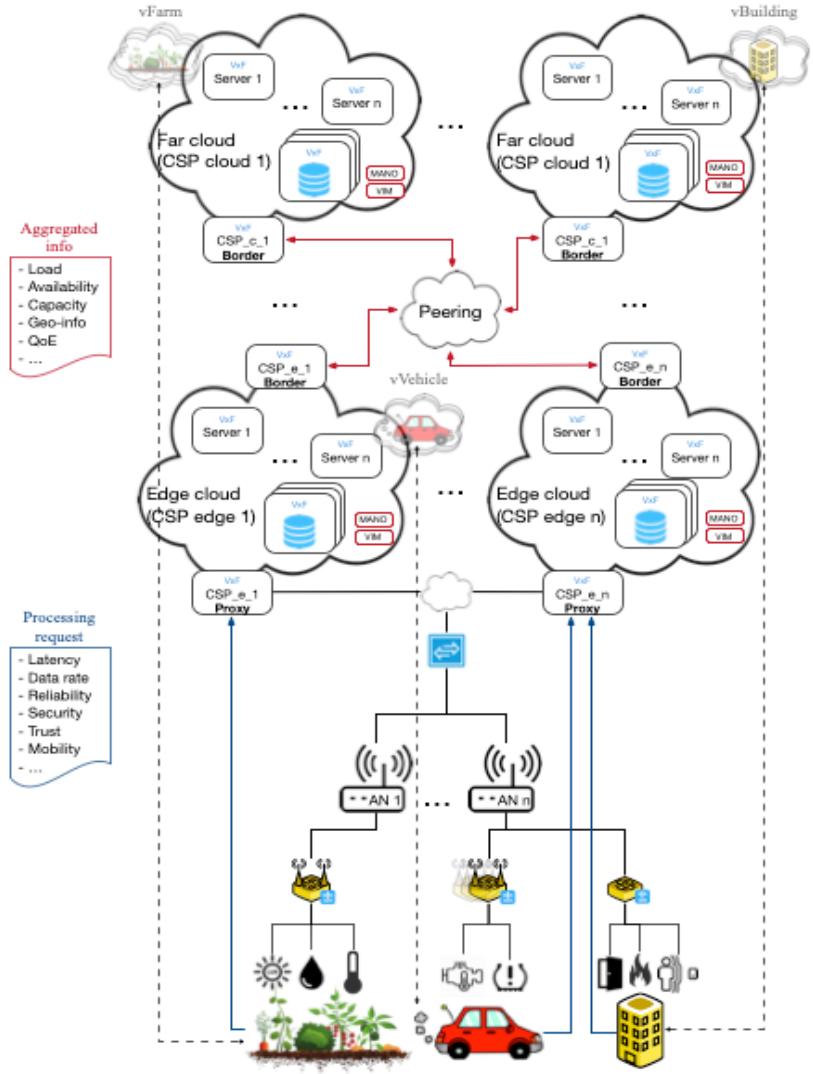




- 5G as infrastructure for flexible processing distribution
- Dynamic management of resources through virtualization

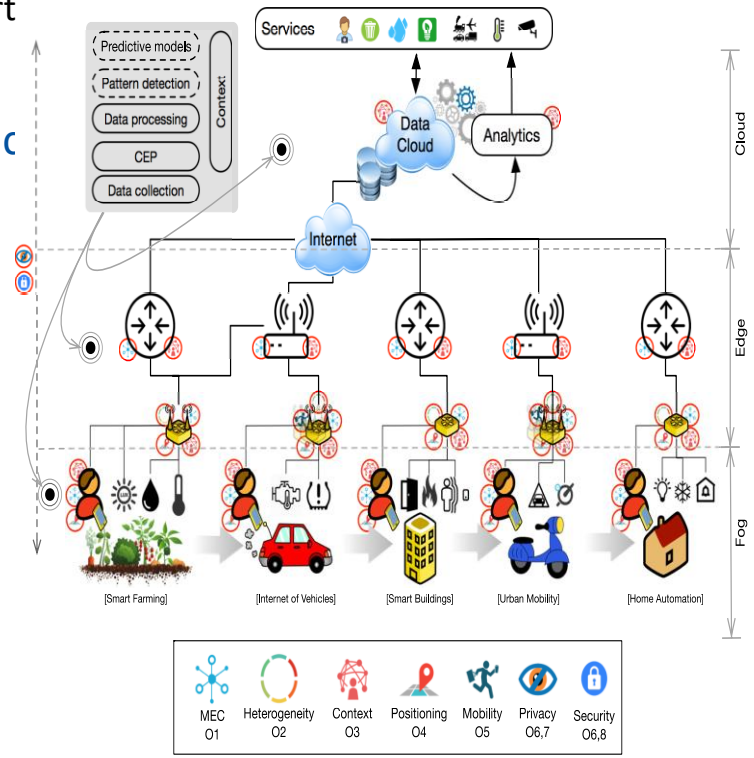
Research and Innovation priorities - a look ahead

- Intelligent methods to optimize the offload processing operations to the proper levels of the computing continuum
- Distributed model for assigning computing resources
- Increase embedded intelligence on IoT devices
- Active and adaptive security within:
  - IoT lifecycle
  - Mobility and transition of the devices
- (ML) techniques can be key for a more effective detection and mitigation of security and privacy attacks
- Contextual management and reactive adaption



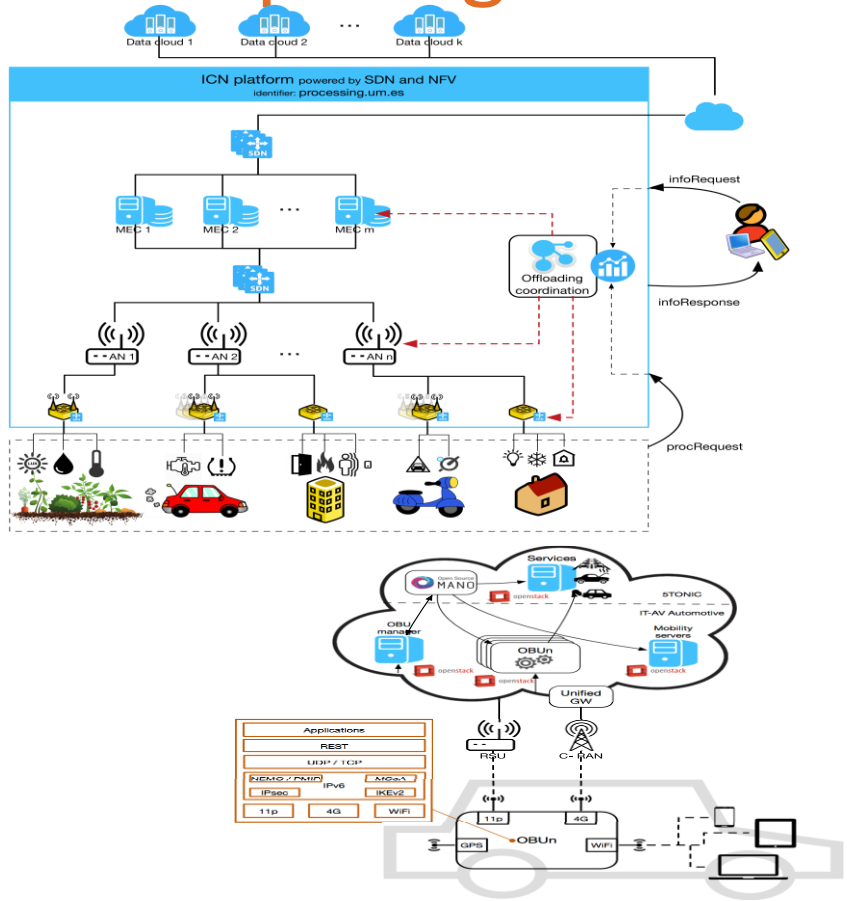
Spreading Computing

- Lower and upper edges of the network need **computing offloading:**
  - **End devices** with energy constraints: IoT hardware, smart phones, sensors…
  - **Cloud data centres** can suffer from scalability issues
- **Exploit MEC** for delay-sensitive services, instead of c computing: one of the main focus of 5G
  - MEC reduce delay when accessing telematic services
  - Processing in the access network
  - Intermediate solution between edge and cloud schemes
  - Under standardization (ETSI, 3GPP)
- **Context-awareness** in processing distribution
  - Use of contextual data to adapt processing
  - Adaptation of the networked system according to the user/network context
- Exploitation of **pre-processing** in MEC/fog/edge computing
  - Filtering, aggregation, event extraction
  - Offloading high levels of fine-grain data analysis



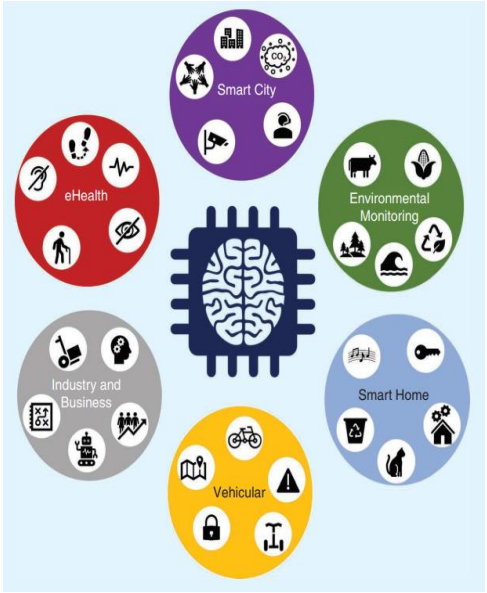
Distributed Computing Resources

- Application of **AI techniques** for dynamic distribution of computing
  - Machine learning to extract computation patterns in the network
  - Predictive adaptation of the processing resources
  - Distributed AI for network adaptation: agents
- **Migration of computing nodes**
  - Movement of virtualized resources to accommodate computing needs
  - Computing nodes “follow” physical devices in the network topology
- **Vertical and horizontal coordination**
  - Vertical: from the end-node to the cloud
  - Horizontal: across a network level (end-nodes, network gateways, access networks, data clouds, etc.)



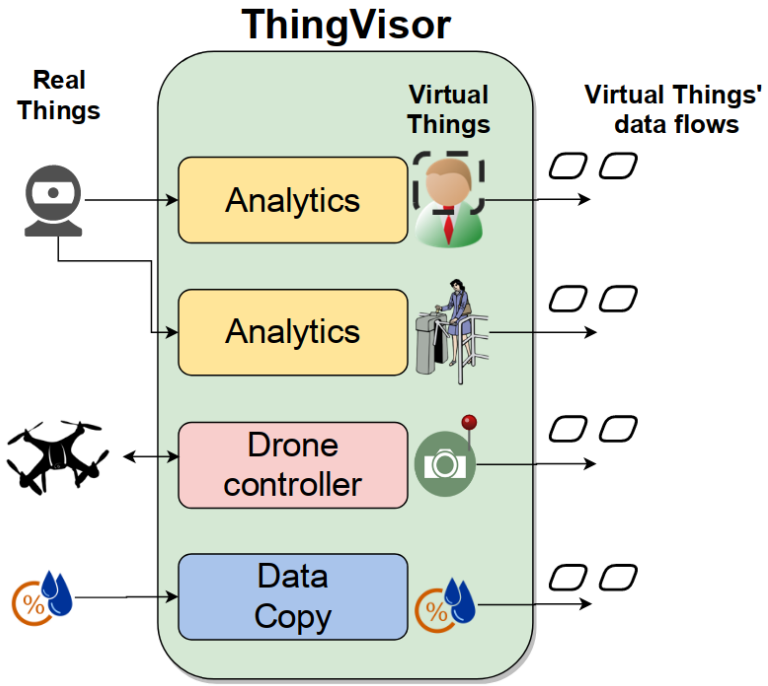
TinyML advantages

- TinyML proposes to optimize and compress ML models in order to make them runnable by small IoT devices
- On-device data processing presents a series of advantages:
  - Local intelligent decisions can be made without the support of the cloud
  - Reduce the amount of data sent to the cloud:
    - Decrease energy (battery) consumption: Wireless transmissions are highly power-demanding
    - Data privacy/security is improved
  - Low cost: Devices are already deployed and they are cheap
  - Reduce latencies in the decision process

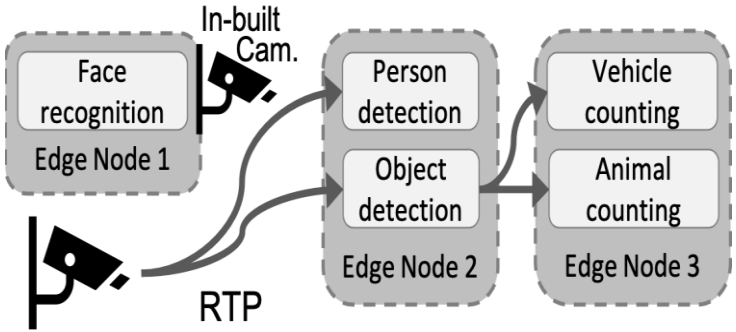


Virtual Things

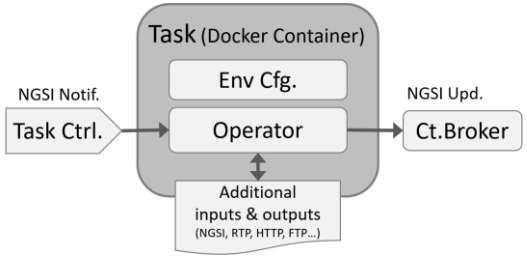
- VirtualThings are **emulation of real things**
  - Sharing of real things
  - Analytics
  - Physical Control
- Virtual **Sensors**
  - Virtual Face Detector
  - Virtual Person Finder
  - Hygrometer
- Virtual **Actuator**
  - Rented Drones
  - Door locks

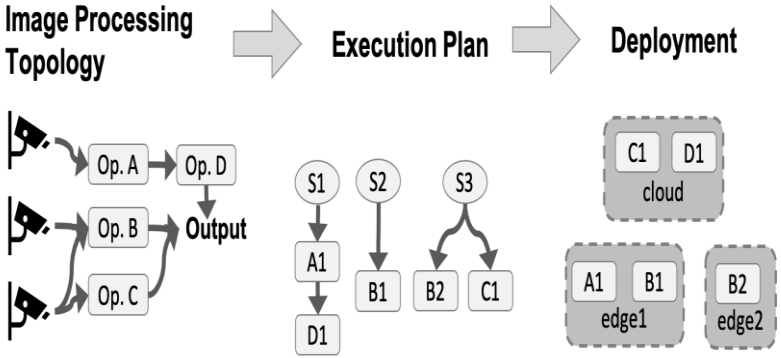


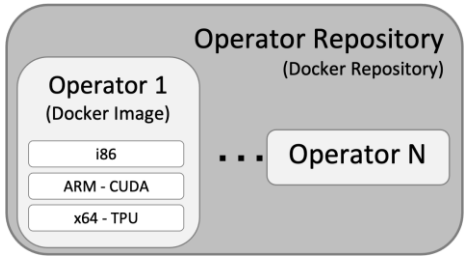
Offloading and distributed processing



- Several image processors may use DNN Pre-Trained Models and can be also orchestated
- Several instance can be available, i.e the operator can be implemented using CUDA acceleration to speed up the process and reduce the energy use.



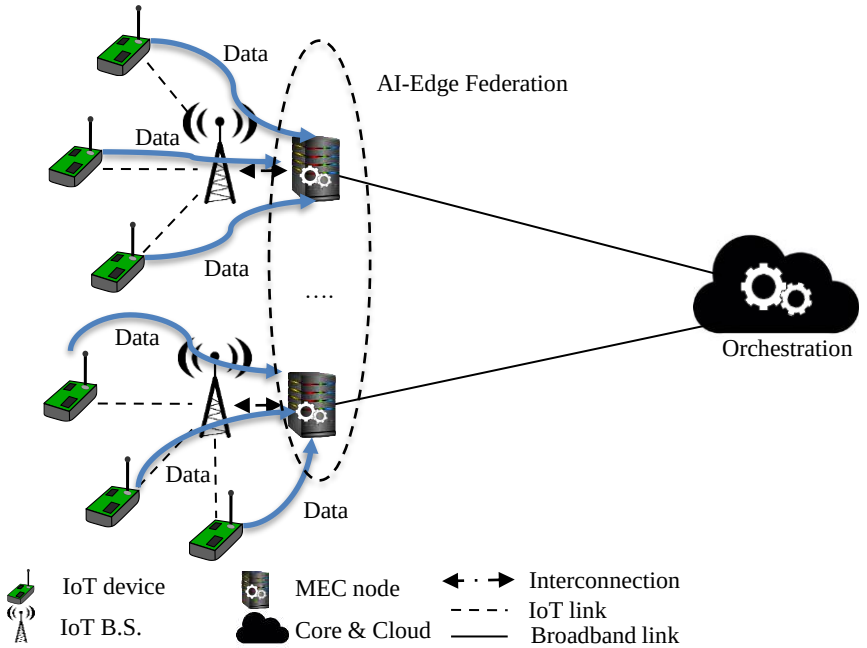




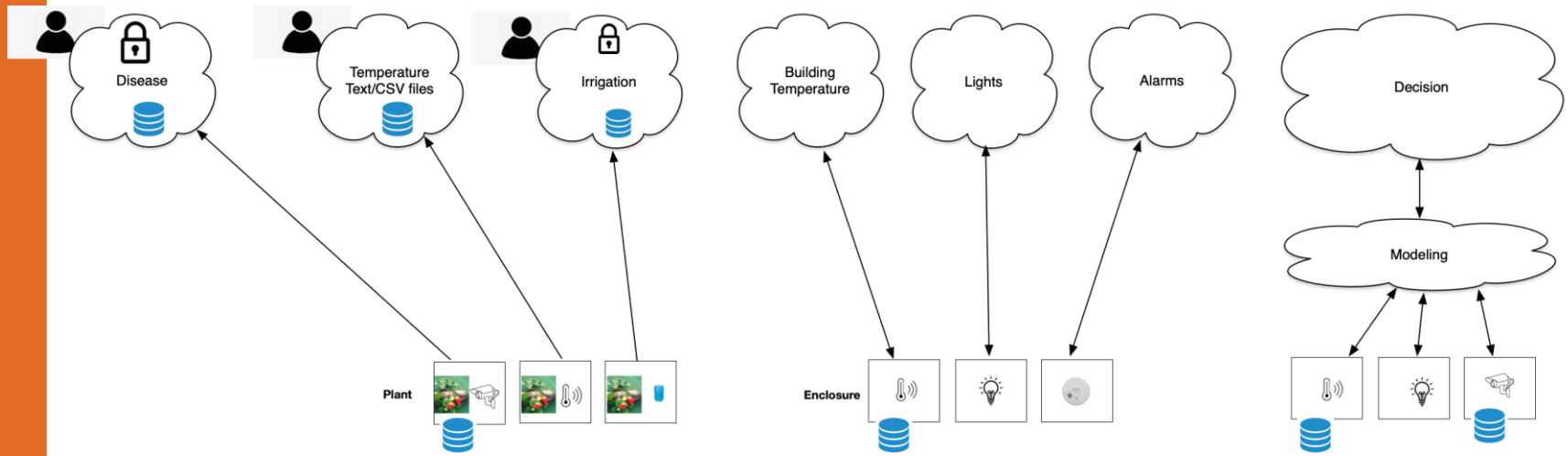
MEC Federated learning

- Coordinated MEC nodes for AI operations
- Cooperative model building, data privacy, etc.

- Typical Intrusion Detection Systems (IDS) are based on centralized approaches, where devices need to share their data with the data center for further analysis
  - It could represent a privacy concern In IoT scenarios where devices' network traffic could disclose users' daily activities
- FL represents a collaborative learning approach where devices share their data, only share partial updates

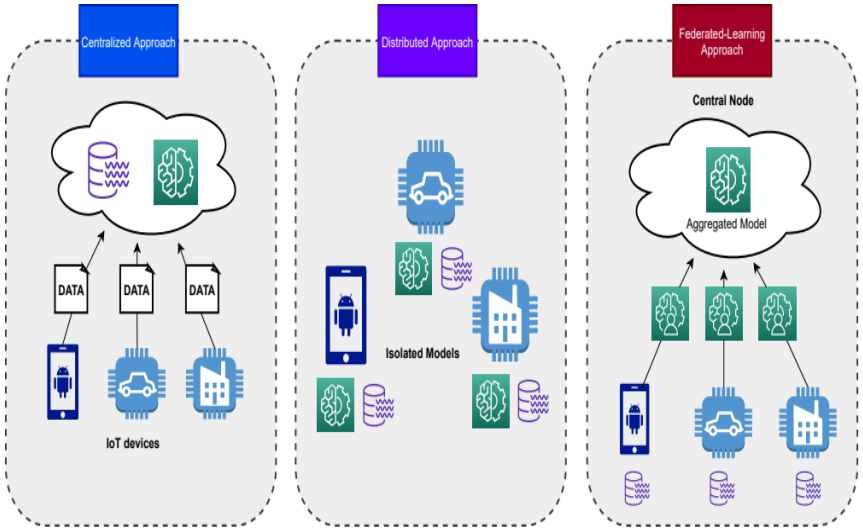


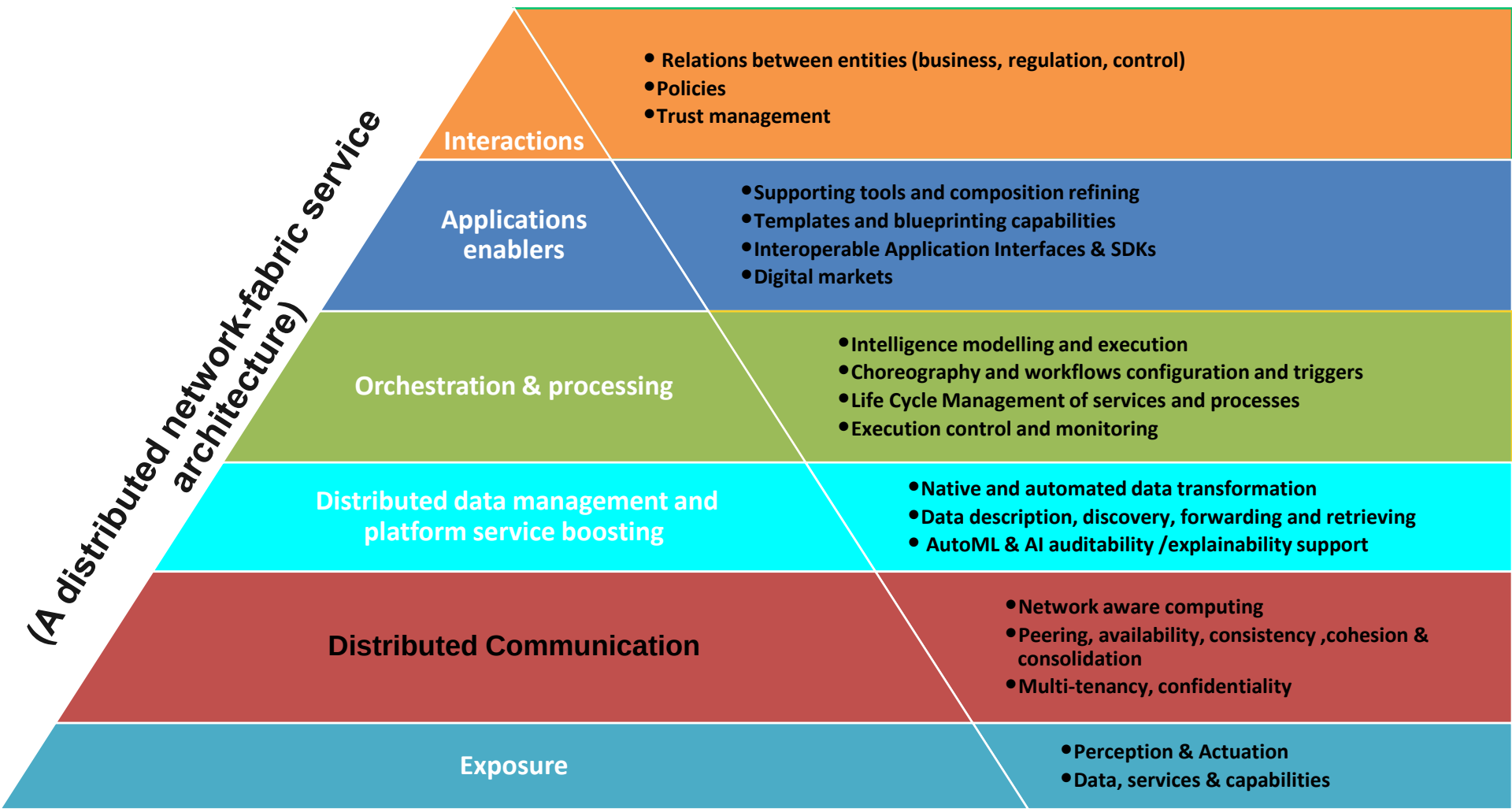
IoT today a fragmented verticalized world -



Federated Learning for Intrusion Detection

- Typical Intrusion Detection Systems (IDS) are based on centralized approaches, where devices need to share their data with the data center for further analysis
  - It could represent a privacy concern In IoT scenarios where devices' network traffic could disclose users' daily activities
- FL represents a collaborative learning approach where devices share their data, only share partial updates

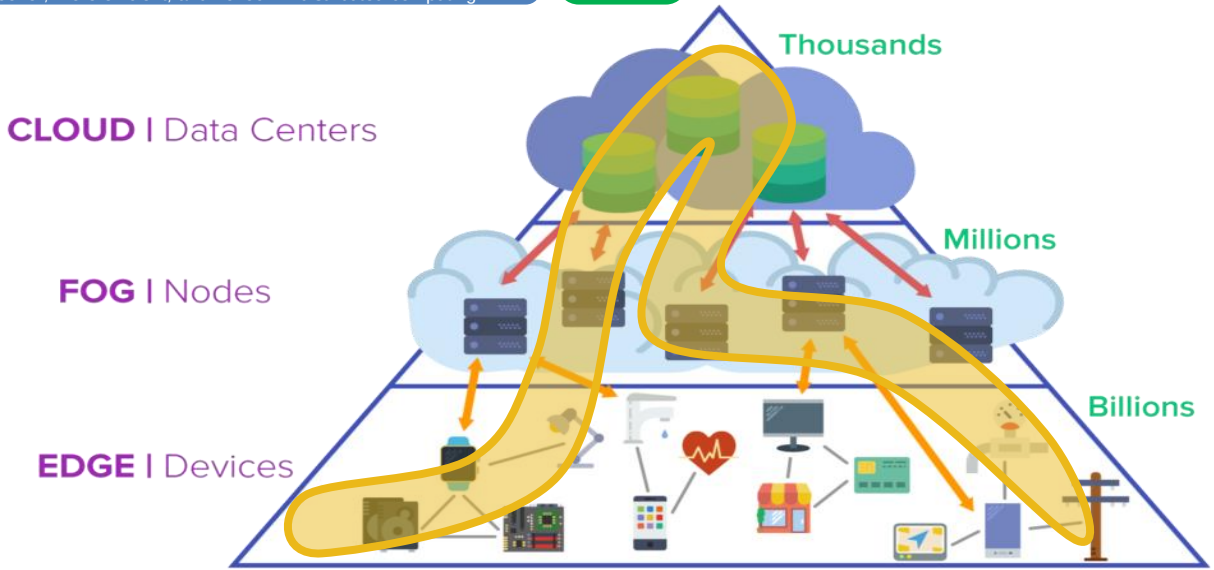



(A distributed network-fabric service architecture)
Interactions
Relations between entities (business, regulation, control)
Policies
Trust management
Applications enablers
Supporting tools and composition refining
Templates and blueprinting capabilities
Interoperable Application Interfaces & SDKs
Digital markets
Orchestration & processing
Intelligence modelling and execution
Choreography and workflows configuration and triggers
Life Cycle Management of services and processes
Execution control and monitoring
Distributed data management and platform service boosting
Native and automated data transformation
Data description, discovery, forwarding and retrieving
AutoML & AI auditability /explainability support
Distributed Communication
Network aware computing
Peering, availability, consistency ,cohesion & consolidation
Multi-tenancy, confidentiality
Exposure
Perception & Actuation
Data, services & capabilities

FLUIDIFY THE CLOUD-EDGE

Create a substrate where your application simply works, somewhere, in the best location.
Simplify applications deployment and management. Make better use of available resources. For a greener, more efficient, and no lock-in distributed computing.

Additional (orthogonal) dimension: capability to handle multiple administrative domains.



APPROACH

1. **Fluidify the edge and unify it** with the cloud through a borderless, decentralised continuum leveraging automatic, autonomous resource discovery and integration.
2. Move the gravity outside the data centre thus creating a cross-provider, community-based computing and service fabric leveraging open-source software.
3. Orchestrate services and hyper-distributed applications in a continuous, automated fashion over multiple devices and domains, leveraging energy-efficient learning algorithms and AI for mobility/behaviour prediction and traffic forecasting.
4. Introduce a Zero Trust paradigm aimed at securing the access of geographically scattered resources in an authenticated, authorised manner.

- Reduced costs
- Increased agility in software development and deployment
- Reduced energy consumption
- New business pathways

kubernetes

Open Source implementation of FLUIDOS
Influencing key OS communities in the area

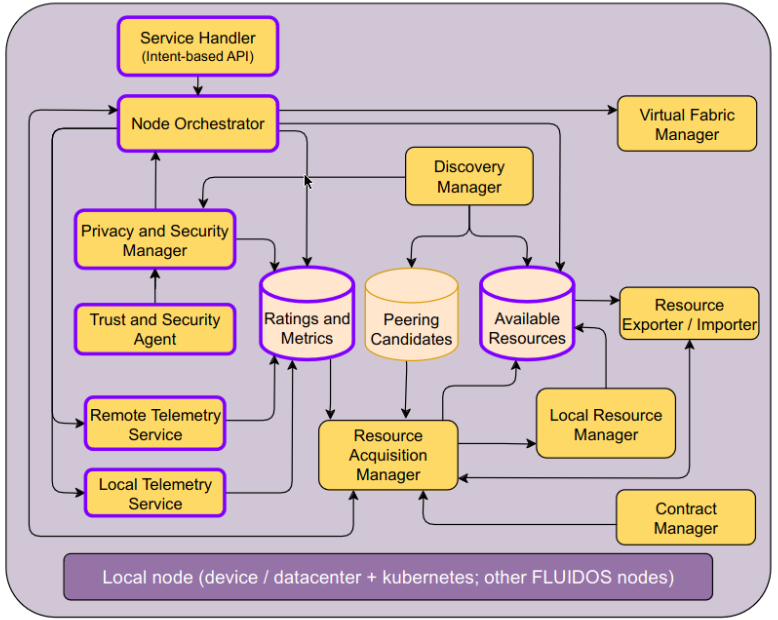
A vibrant community of early adopters
Embracing new paradigms toward edge-native computing

Security Challenges

- **The Cloud Computing paradigm has been growing** as well as the demand for storage and processing
- **New paradigms** have emerged such as **Fog/Edge/Micro-Edge computing**, with the goal:
  - Release the Cloud
  - Privacy
  - Latency
  - Security
- At the Edge, **we find heterogeneity** so it's necessary **mechanism of orchestration** of services **across multiple layer** keeping the security

Framework Overview

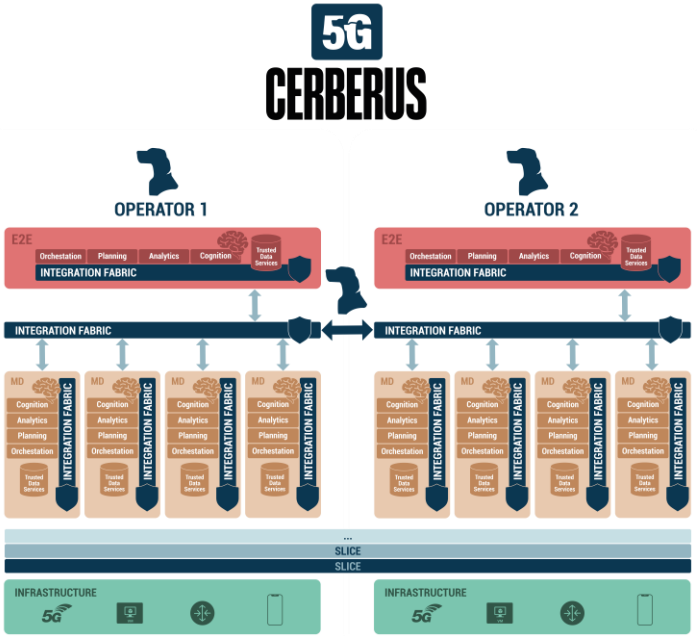
- **FLUIDOS** (Flexible, scaLable, secUre, and decentralIseD Operating System)
- It is a research project that **aims to create a decentralised operating system** that unifies **distributed** node **resources** and **capabilities** under a homogenised view
- The system allows the deployment and management of services while ensuring their requirements and constraints are met
- **Each FLUIDOS node** can **provide** and **offer** any **resource or service**



Highlighted the components used in this work

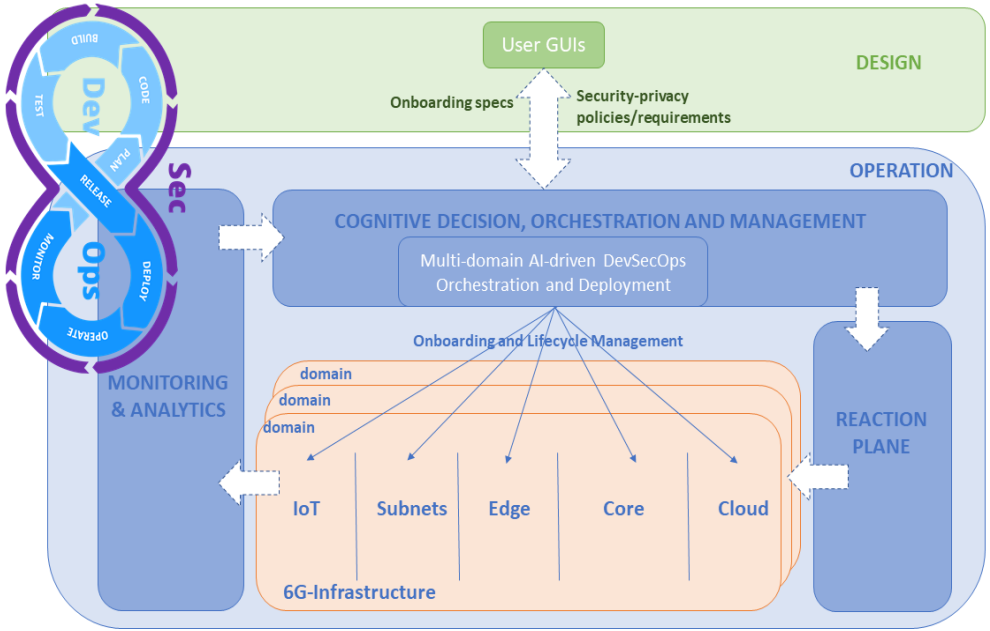
CERBERUS Orchestration on a descentralised Operating System

- **Security Orchestration involves** the coordination of security tools and processes, resulting:
  - **Improved security** posture
  - **increased efficiency** reduced human error
  - **faster response** times
- **Depending on the subject who triggers the orchestration process** and the main goal, the workflow can be separated into two different approaches
  - **Proactive**
  - **Reactive**



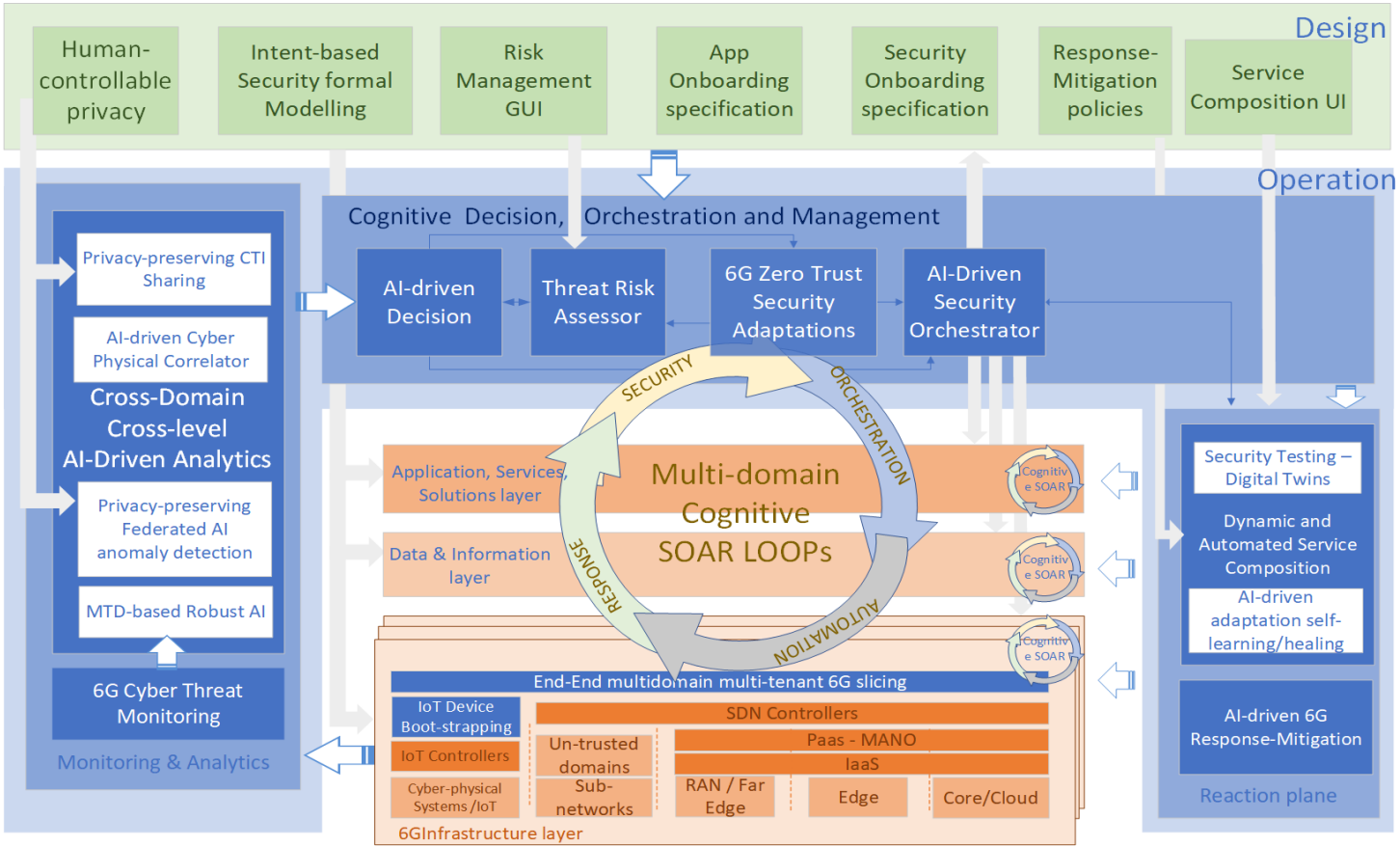
Introduction

RIGOUROUS will introduce a new holistic and smart service framework leveraging new machine learning (ML) and AI mechanisms, which can react dynamically to the ever-changing threat surface on all orchestration layers and network functions.



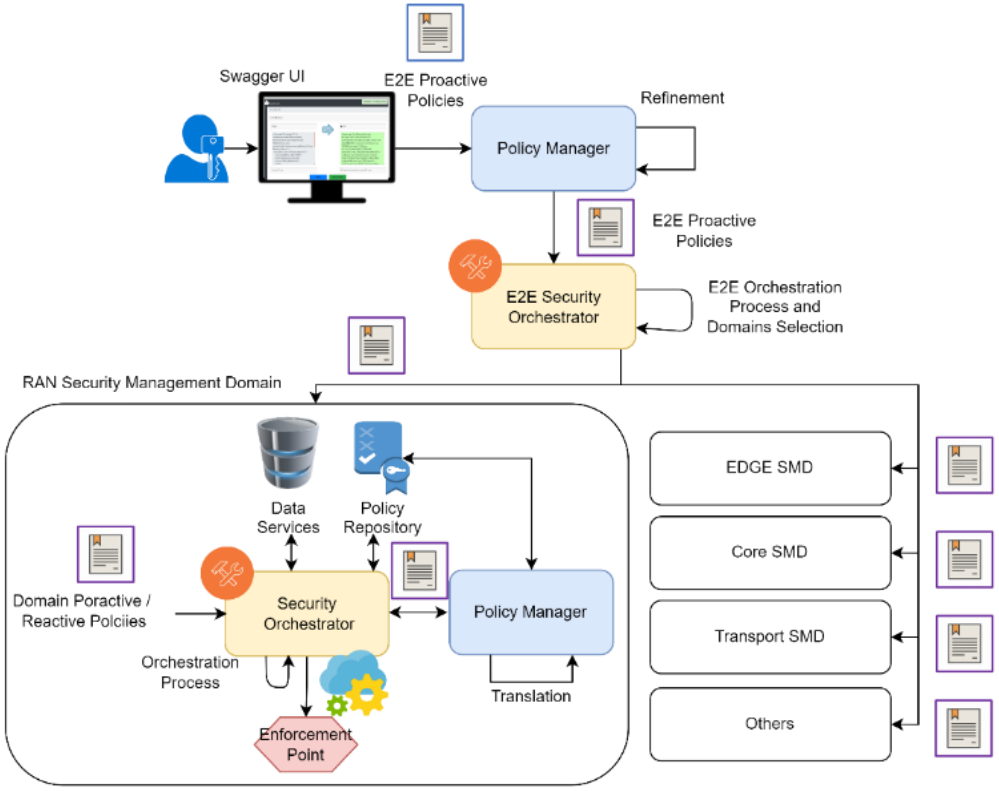
Smart service framework is capable of ensuring a **secure, trusted and privacy-preserving** environment for supporting the next generation of trustworthy continuum computing 6G services along the full **device-edge-cloud-continuum on heterogenous multi-domain networks**. This includes establishing compliance with the design of software (SW), protocols and procedures, as well as AI-governed mechanisms to cope with the security-related requirements in the **full DevOps lifecycle**, from the service onboarding up to the day-2 operations.

High-level Functional Architecture



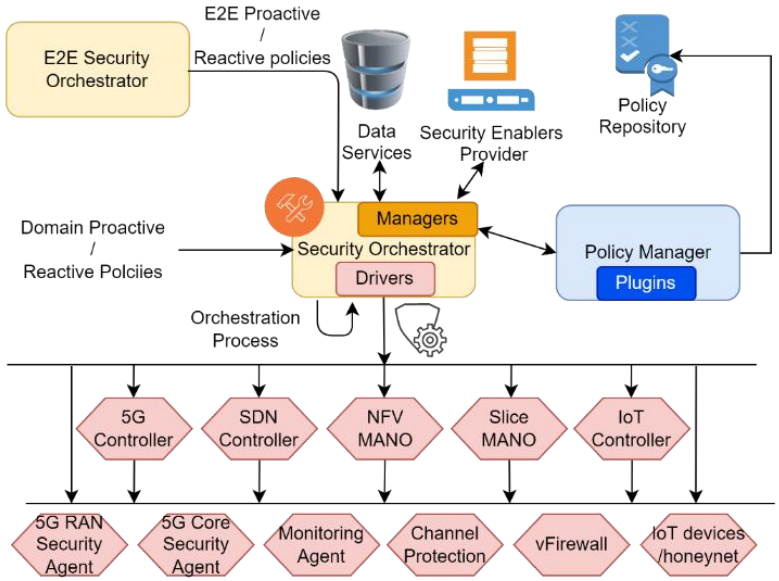
Policy-based AI-driven Security orchestration

- User intent driven security policy definition
- The orchestrator will be driven by AI to make their chaining and orchestration decision
- Rely on special modules to translate the intents, policies and behavioural profiles coming from the decision into concrete actions
- **Federated Learning (FL)** approach to make orchestration decisions
- Decide best actions for **dynamic** provisioning, deployment, and **reconfiguration** (during operation) of the virtual network security functions and associated intents and policies
- Orchestrator will consider the time- and space-varying parameters of the network, such QoS capacities, actual resources constraints (CPU, RAM, storage), system status, current deployed policies, and threat incidents…

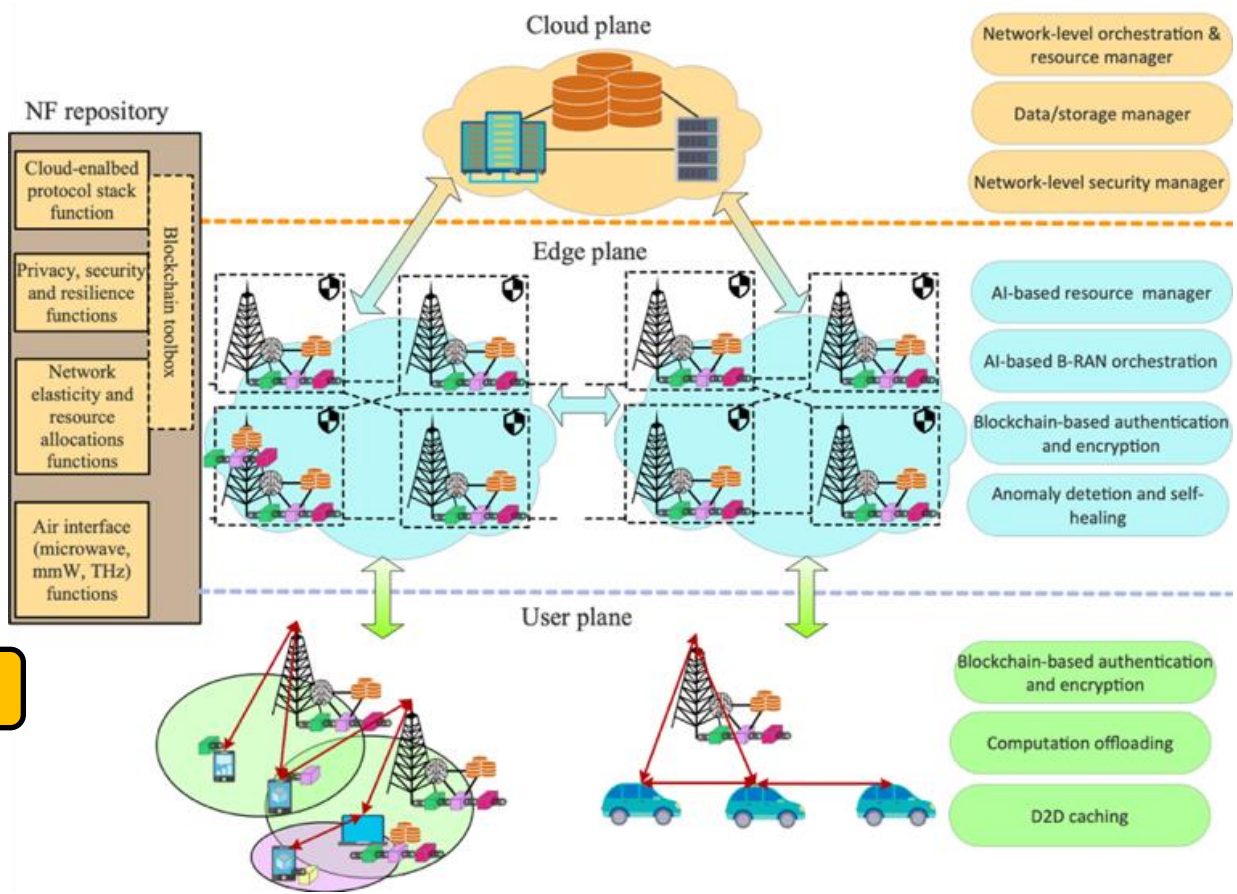


Security enforcement

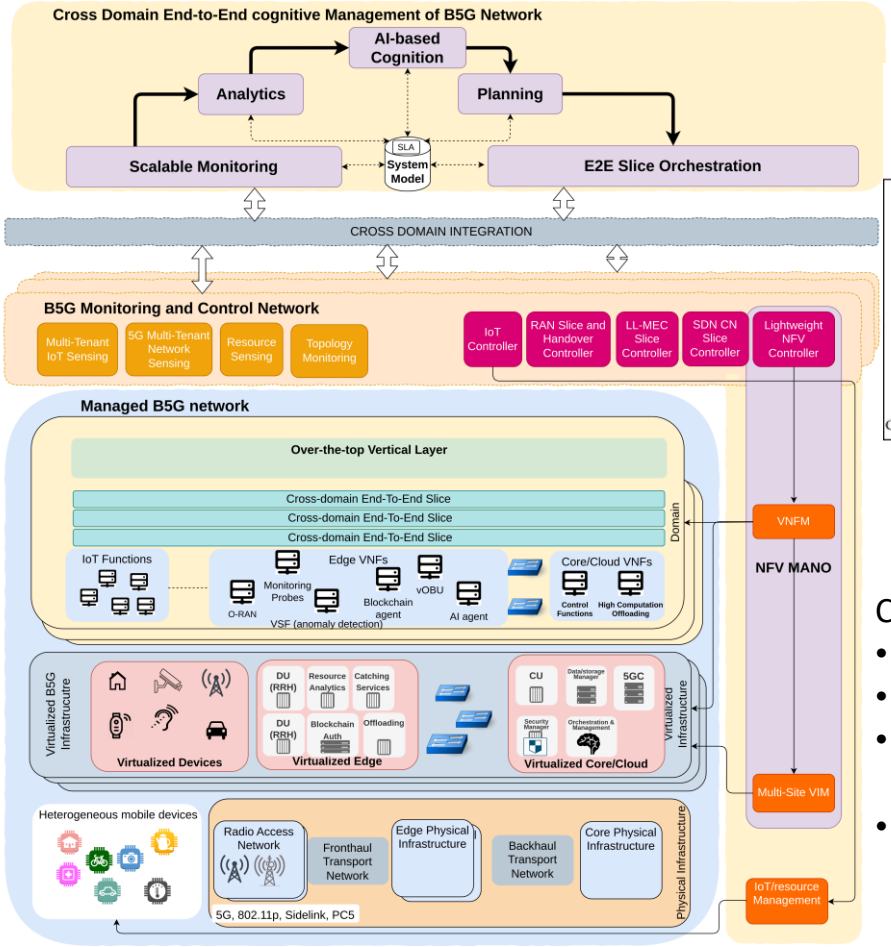
- Extensible orchestration enforcement:
  - NFV, SDN, IoT Controllers
- Integration with Security Enabler Providers (to enforce actions) and Trust Managers to make decisions
- ZSM approach

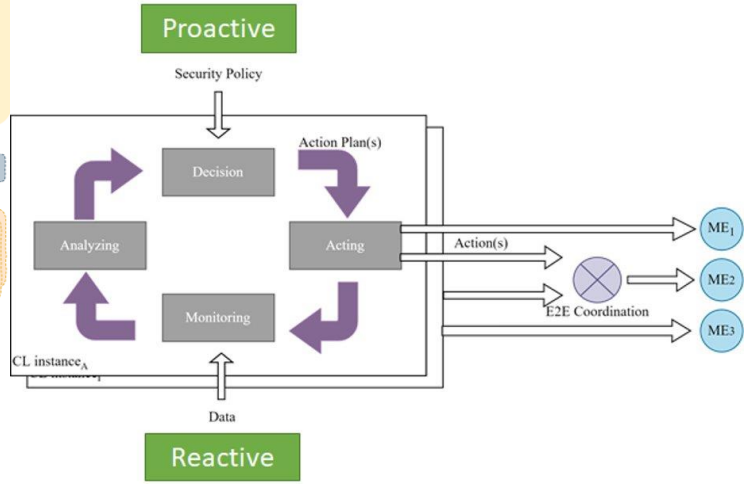


NANCY's Architecture B-RAN



Computational Offloading

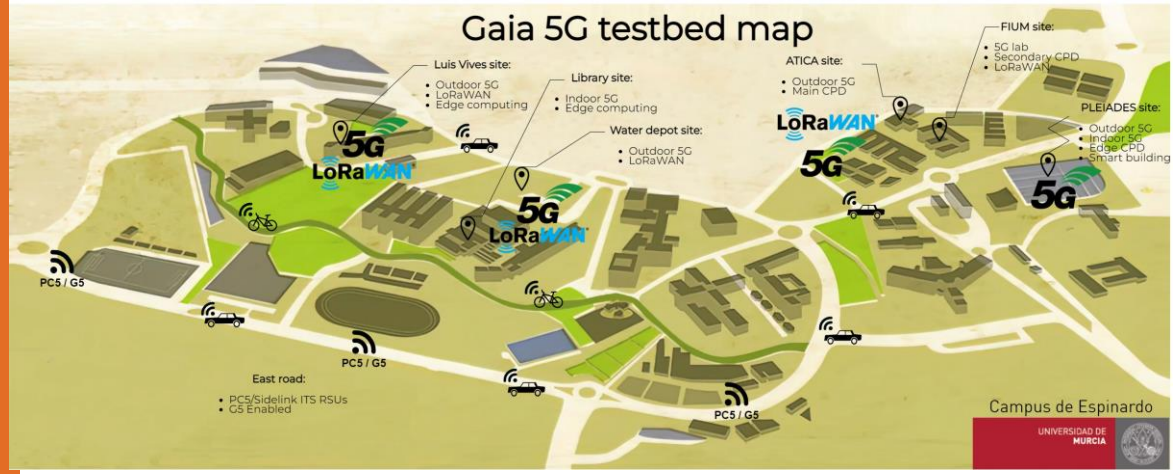


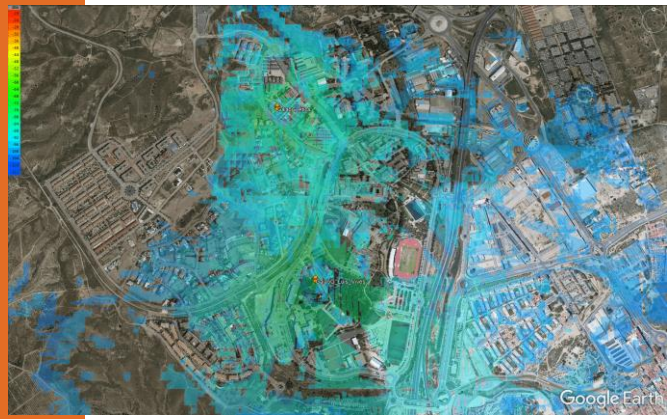


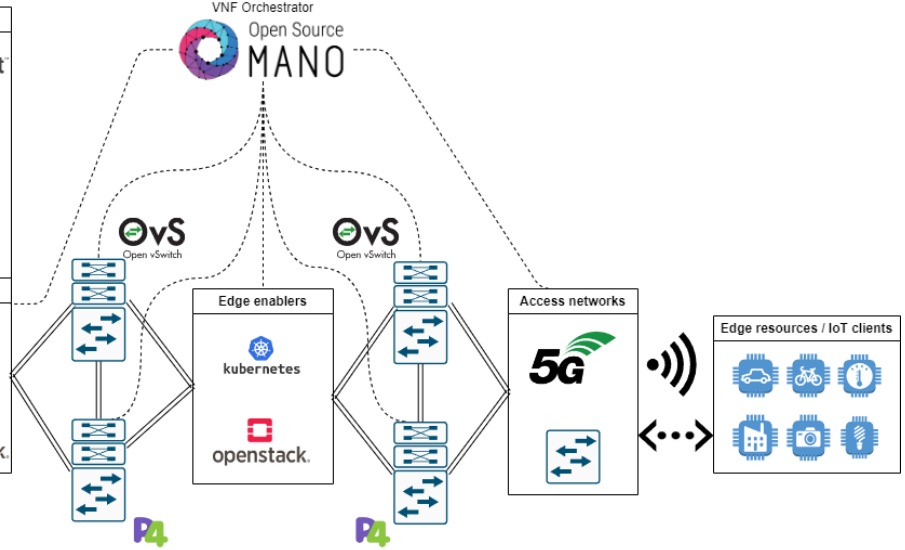
Closed-loop based orchestration:

- Infrastructure/services monitoring
- IA Analytics and predictions
- Orchestration Scheme --> offloading/caching placement
- Instantiation & Configuration

testbed GAIA campus



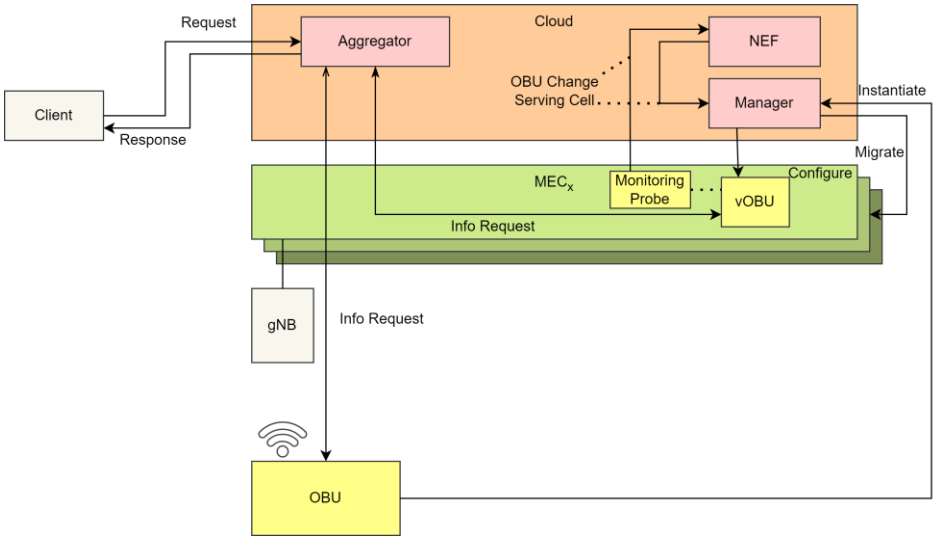


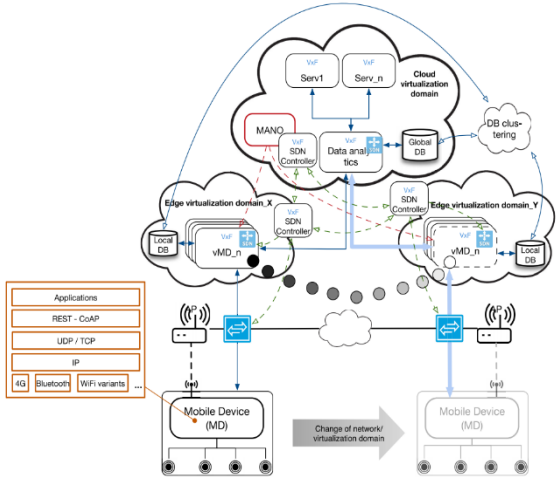


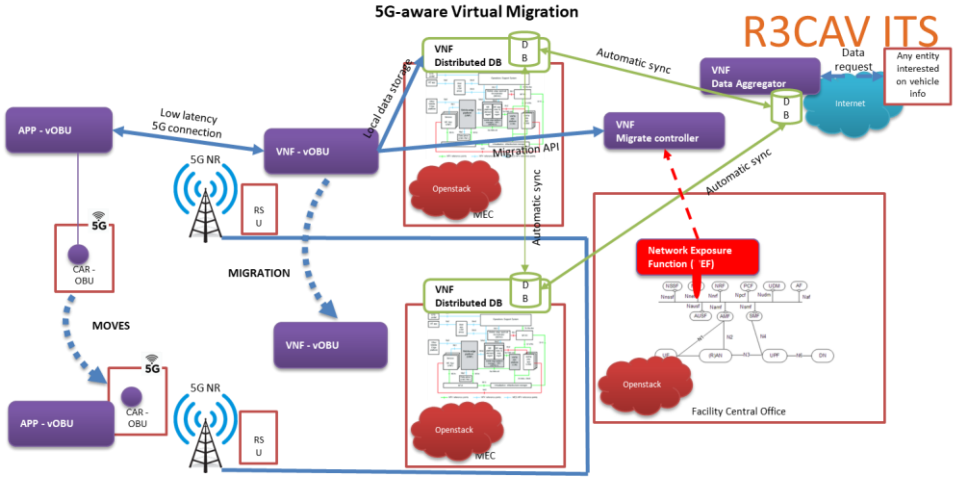
Unión Europea

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

vOBU migration







Conclusion

- AI within devices is just the first step towards the development of completely intelligent and evolutive systems.
  - Integration of cognitive self-evolution capabilities in the entire end-to-end network chain (fog, edge, and cloud) will go beyond current limits of AI by permitting end-devices and, by extension, the whole system to grow and refine its own intelligence
- Security VNFs can be timely and dynamically orchestrated through policies to deal with heterogeneity demanded by these distributed IoT deployments, than can be deployed either at the core of at the edge, in VNF entities, in order to rule the security in IoT networks
- Dynamic and intelligent reactive provisioning of services and resources with the edge of the network can enhance scalability, necessary to deal with IoT scenarios
- Continuum merging IoT/far edge/edge/cloud is opening new challenge on how to coordinate the managing of the resources and how the security and privacy can be managed in this dynamic scenario -> Zero trust

- Evolutive Artificial Cognitive Capabilities (EACC) mechanisms will open the door for designing devices and systems with a superior intelligence that will permit them to meta-learn from new situations, scenarios, and environmental changes.

Acknowledge

RIGOUROUS has received funding from the European Union's HE Research and Innovation Programme HORIZON-JU-SNS-2022 under Grant Agreement No 101095933 https://rigourous.eu/

The FLUIDOS project has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No 101070473

R3CAV project is funded by CDTI and the Spanish Ministry of Science and Innovation

CERBERUS has received funding from Spanish Ministry of Economic Affairs and Digital Transformation and the European Union's NextGenerationEU under Grant Agreement TSI-063000-2021-36, 44, 45 and 62