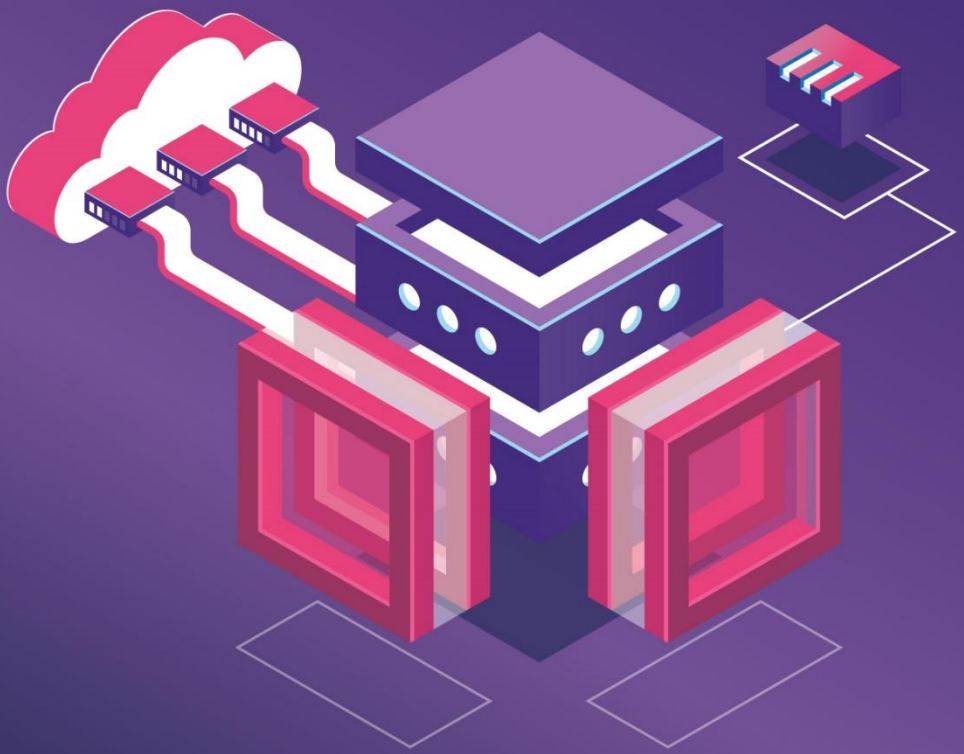
EUCloudEdgeIoT.eu
Open Continuum

Compositional view of the Continuum Reference Architecture

Graphical representation of common, and potential, capabilities

Authors

This work was performed by Task Force 3:
Architecture leader, part of the OpenContinuum project consortia, within the EUCloudEdge initiative.



Grant Agreement No.: 101070030 **Topic:** HORIZON-CL4-2021-DATA-01-07
Call: HORIZON-CL4-2021-DATA-01 **Type of action:** HORIZON-CSA

CONTENTS

Funded by Horizon Europe Framework Programme of the European Union

1. INTRODUCTION

This is the last document of a series of 3 for designing a Reference Architecture for the continuum. The first document of the series presented an initial version of a common taxonomy, considering it as a unified language for all actors of the value chain. It also introduced the initial set of building blocks that set the basis for the development of the architecture. The second document of the series drafted the functional view, including the minimum set of functionalities needed to address the cloud, edge and IoT requirements for managing the lifecycle of a service application across the continuum. closer to the edge.
With the contributions of different EU research funded projects, tackling gaps from different perspectives, the final view of how the architecture should look like was finally defined.
This paper presents graphic representation of the compositional view of the Reference Architecture, easily readable and interpretable, so it can be further reused by different actors implementing it into their own solution architecture addressing their specific needs.

ABOUT THE AUTHORS

This work was performed by Task Force 3: Architecture leader, part of the OpenContinuum project consortia, within the EUCloudEdge initiative.
Task Force 3 aims to provide a common vision on Continuum computing, providing a homogenised language and a reference architecture to set the basis for a European standard, positioning Europe ahead of the competition. The work presented here has been further validated with 30 ongoing research projects in the fields of edge, cloud and IoT (mainly ICT-40-2020, ICT-50-2020, ICT-56-2020, HORIZON-CL4-2021-DATA-01-05, HORIZON-CL4-2022-DATA-01-02, HORIZON-CL4-2022-DATA-01-03, HORIZON-CL4-2022-DIGITAL-EMERGING-01-26 and HORIZON-CL4-2023-DATA-01-04) and will be extended in the coming months until the reference architecture is mapped with all projects' solution architectures.

Funded by Horizon Europe Framework Programme of the European Union

2. HOMOGENISED VIEW OF THE REFERENCE ARCHITECTURE

As a result of the previous work, a set of components implementing the identified functionalities were designed. In this way, a graphical representation can be provided simplifying the understanding of the presented concepts. Some projects, as well, are mapping their own architectures with this common one highlighting the commonalities and adding additional considerations that are tailored to their specific needs.

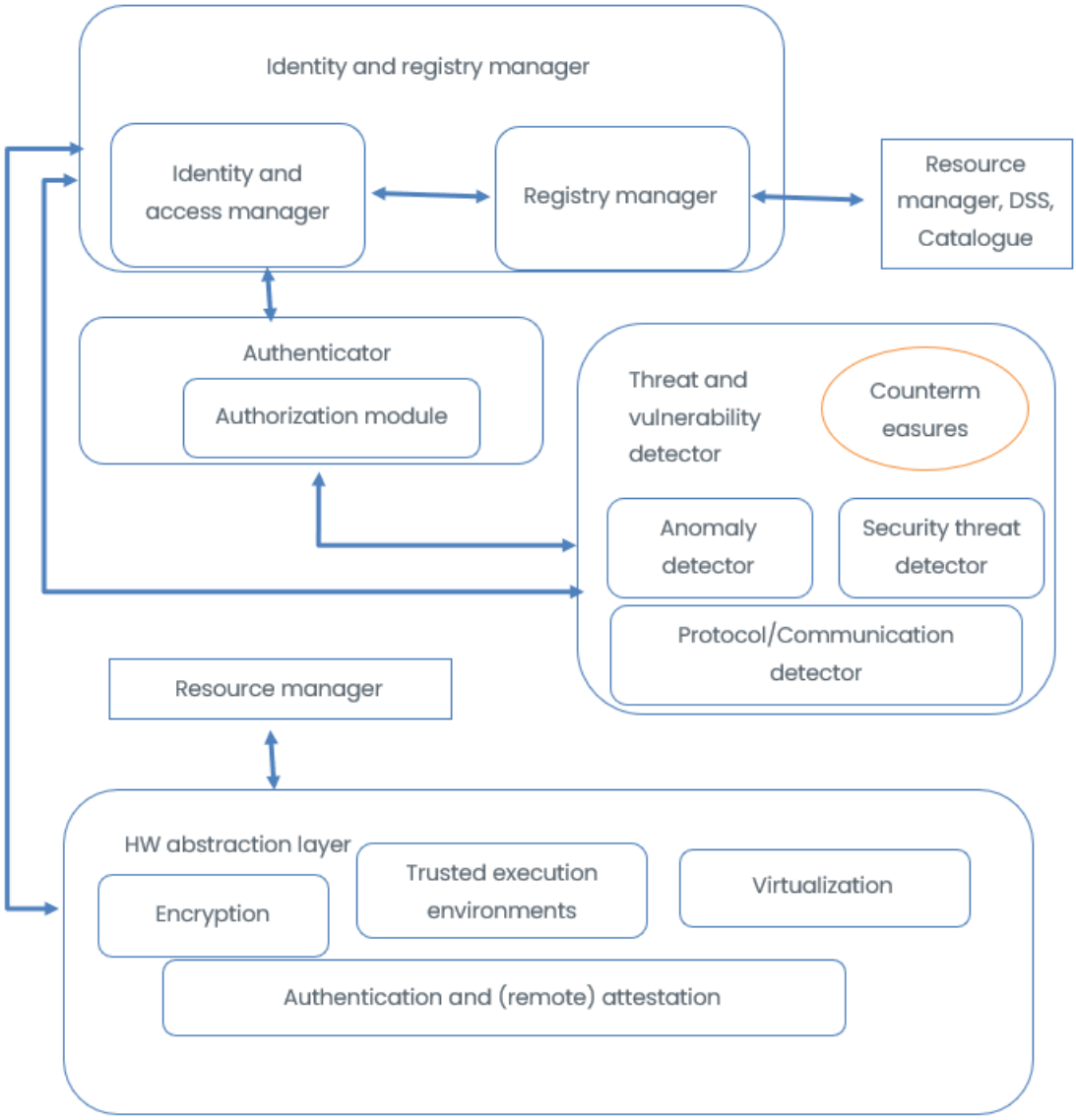
The work presented in the following subsections introduces the basic graphical representation of each of the building blocks to implement the identified minimum set of functionalities. However, the representation is flexible enough to be further extended with the additional functionalities coming from specific research requirements of use cases' needs.

ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
App	Application
BPF	Berkeley Packet Filter
DB	Database
DPU	Data Processing Unit
DSS	Decision Support System
FaaS	Function as a Service
HW	Hardware
IDS	Intrusion Detection System
IoT	Internet of Things
LB	Load Balancer
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
MUD	Manufacturer Usage Description
NAT	Network Address Translation
NFV	Network Function Virtualization
NIC	Network Interface Card
PUF	Physically Unclonable Function
QoE	Quality of Experience
QoS	Quality of Service
SLO	Service Level Object
SW	Software
TPM	Trusted Platform Module
TOPSIS	Threat-Oriented Person Screening Integrated System
UC	Use Case

Funded by Horizon Europe Framework Programme of the European Union

3. SECURITY AND PRIVACY



COMMON CAPABILITIES:

- Identity and registry manager
  - Identity and access manager (for users and HW), using e.g., PUFs and TPMs on hardware level
  - Registry manager
- Authenticator
  - Authorization module
- Threat and vulnerability detector + countermeasures
  - Anomaly detector

Funded by Horizon Europe Framework Programme of the European Union

    - Security threat detector
    - Protocol/Communication detector (includes network connections)
    - Impact analyser & recommender
- HW abstraction layer (for security)
    - Encryption
    - Trusted execution environments - Connected to Trust Calculator
    - Virtualization
    - (remote) attestation - Connected to auth/authorization module

OPTIONAL FOR SPECIFIC UCS:

- Secured transactions (blockchain)
- Accounting mechanisms

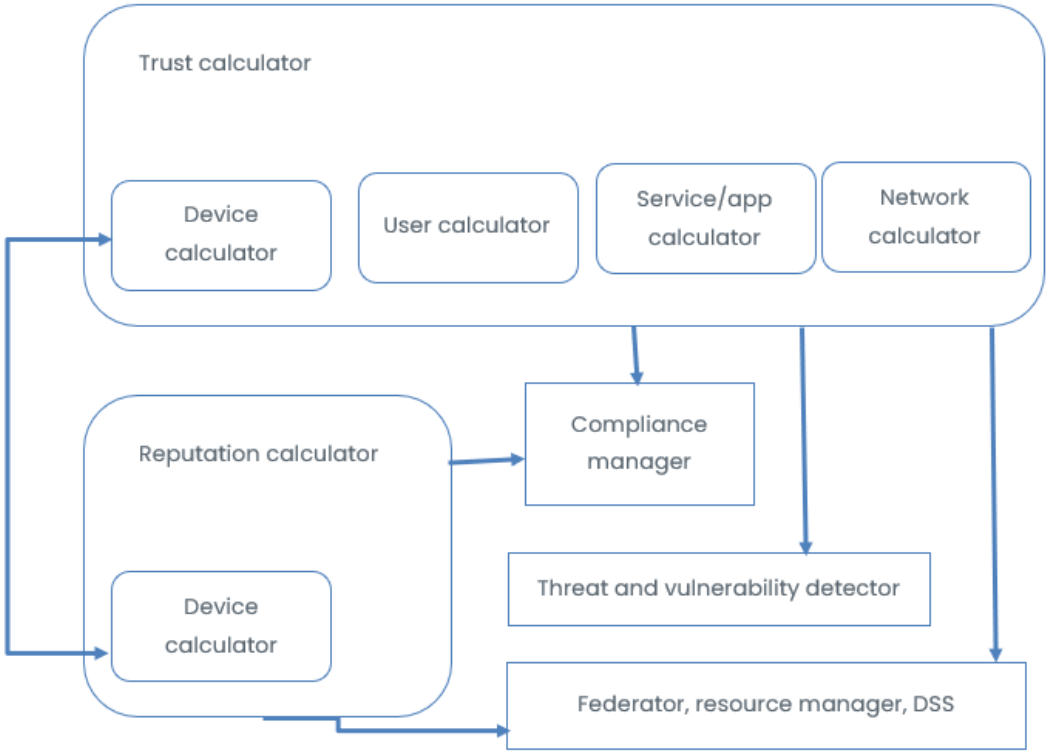
SPECIFIC FOR SAFETY (RELATED TO BUILDING BLOCK 2 – TRUST & REPUTATION):

- Functional safety
- Network measures for deploying ms in different network instances

Funded by Horizon Europe Framework Programme of the European Union

4. TRUST AND REPUTATION

Beyond security, it is needed to implement the necessary mechanisms to measure the trust and reputation levels of the users, providers and any additional source.



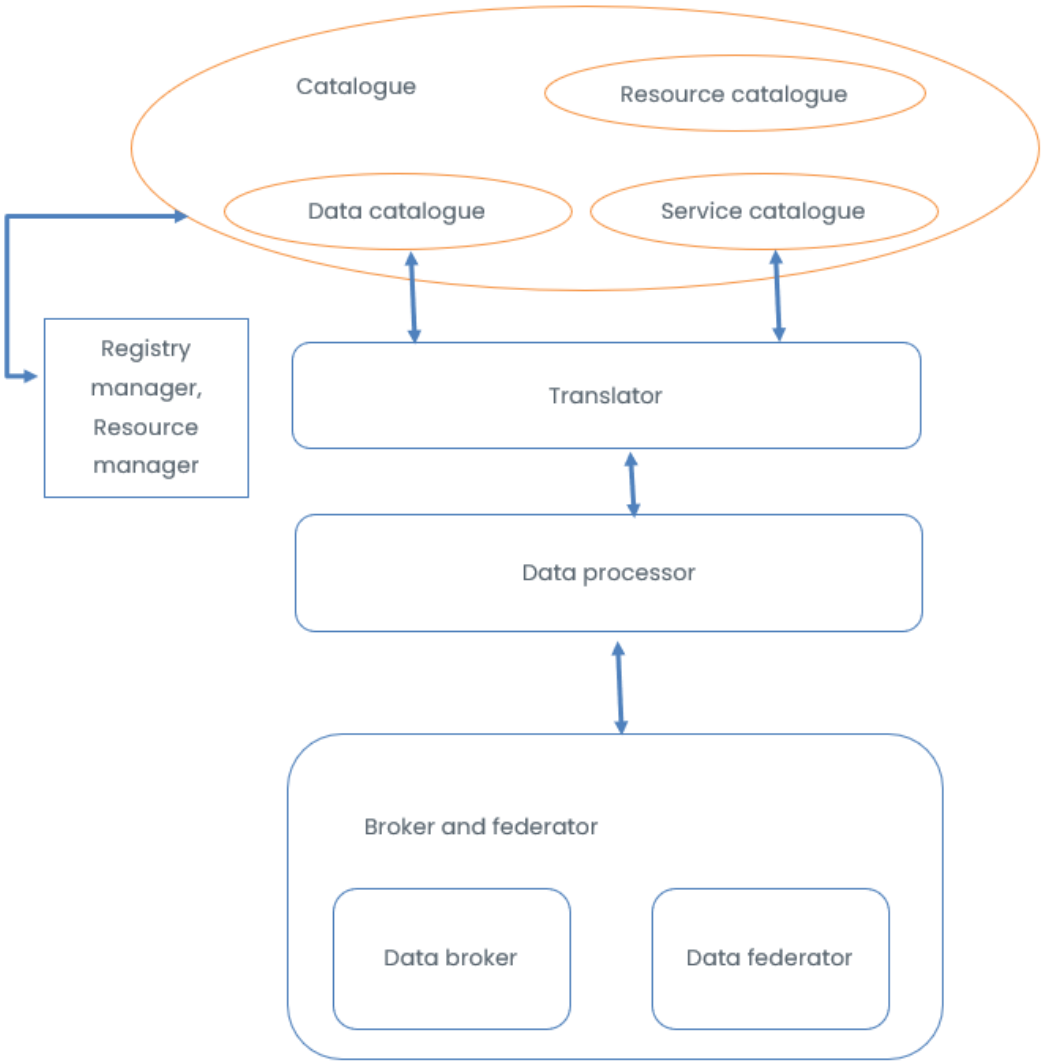
COMMON CAPABILITIES:

- Periodically updated trust score for IoT devices and user trust is needed for security/safety consideration.
- Trust calculator (context-aware - considering parameters from different contexts (e.g., device capabilities, network, app, security…)
    - Calculates trust from the device perspective — user perspective — application/service perspective.
    - Device trust: HW/SW specifications of the manufacturer (MUD protocol)
        - Security capabilities
        - MQTTs or any data brokering protocol.
        - Trust Ranking for recommendation (e.g., TOPSIS, etc.)
            - Inform the user about the trust scores of the current devices capable of offering the service requested.
    - Network/domain trust: IDS, threat intelligence
    - User trust: user behavior, user reputation
- Reputation calculator

Funded by Horizon Europe Framework Programme of the European Union

- HW provider calculator
    - Info to be shared with the user for selecting the most appropriate provider.

5. DATA MANAGEMENT



COMMON CAPABILITIES:

- Data catalogue
    - Data catalogue (streams, APIs, DBs)
    - Service catalogue (for data exposure) – additional
- Data broker and federator
    - Data broker (routing)
    - Data federator - draw connectors blocks

Funded by Horizon Europe Framework Programme of the European Union

    - Connectors (for multiple DBs)
    - Connectors (for multiple data spaces) - challenge: scalability issues (related to data lakes)
- Translator (lowest level to connect DBs) - ensuring interoperability and connected with DR&F, uses data catalogue for information on data models
- Data processor (also providing information for scheduling)
    - Batch processor
    - Stream processor

Optional (not mandatory) / Additional components:

- Backup/Replicas' automated manager (using metadata from data catalogue)

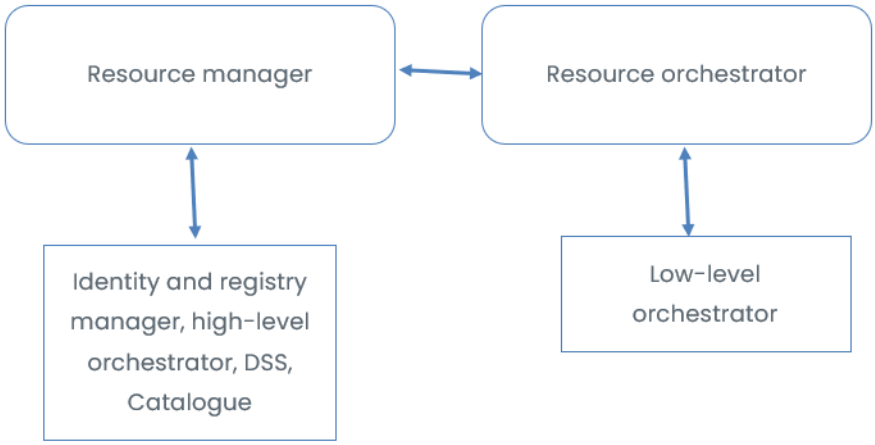
For scheduling data:

- Orchestrating data for analytics

Future research challenges:

- Data lakehouse implementation

6. RESOURCE MANAGEMENT



DEFINITION OF RESOURCE MANAGEMENT

Resource management in cloud, edge, and IoT is the process of efficiently allocating, balancing, provisioning, and scheduling the resources (such as heterogeneous computing power, storage, network bandwidth, etc.) among the different layers of the system to achieve optimal performance, quality of service, energy efficiency, and cost reduction. Resource management techniques can vary depending on the specific characteristics and requirements of each layer and the applications

Funded by Horizon Europe Framework Programme of the European Union

running on them.

Challenges and objectives of resource management in cloud, edge, and IoT are:

- **Scalability:** The system should be able to handle the increasing number of devices, data, and requests without compromising the quality of service.
- **Heterogeneity:** The system should be able to deal with the diversity of devices, resources, platforms, and protocols in the cloud, edge, and IoT layers.
- **Latency:** The system should be able to minimize the delay between the data generation and processing, especially for time-sensitive applications.
- **Reliability:** The system should be able to ensure the availability and fault-tolerance of the resources and services in the presence of failures and uncertainties.
- **Security:** The system should be able to protect the data and resources from unauthorized access and malicious attacks.
- **Privacy:** The system should be able to preserve the confidentiality and anonymity of the data and users in the cloud, edge, and IoT layers.

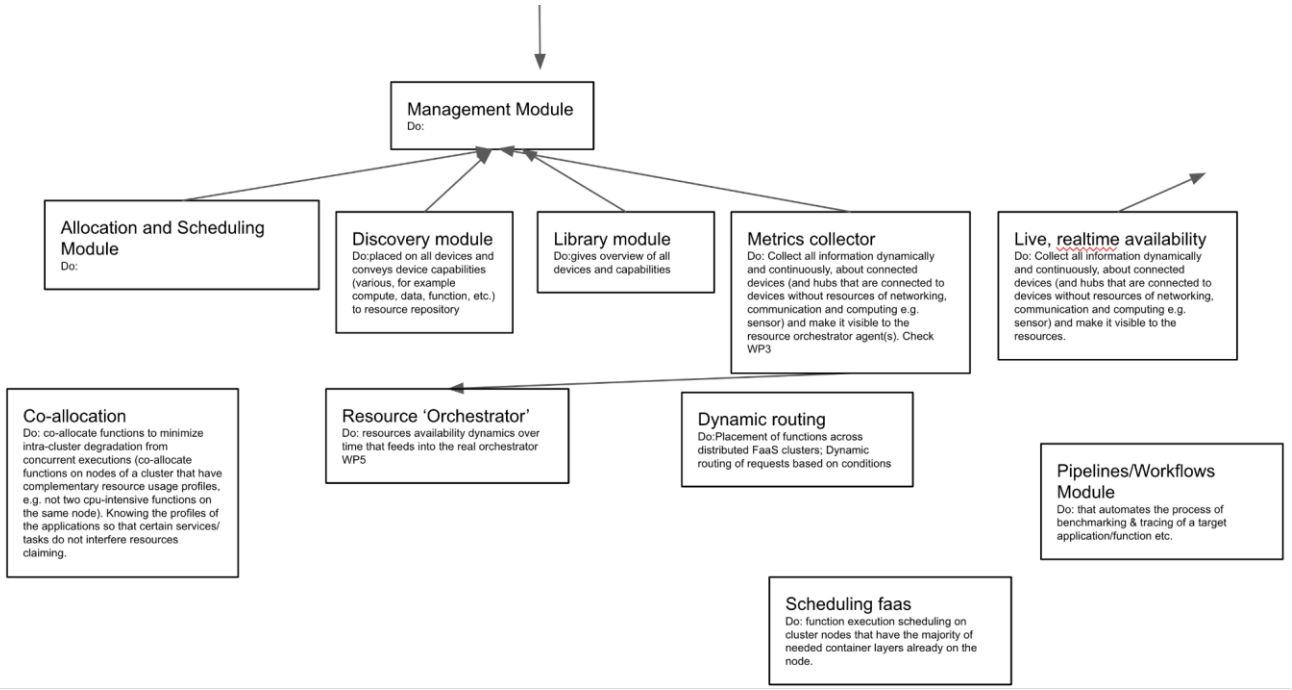
Some of the existing resource management techniques for cloud, edge, and IoT are:

- **Resource allocation:** The process of assigning resources to tasks or applications based on their requirements and preferences. Resource allocation can be done statically or dynamically, centrally or distributedly, deterministically or probabilistically, etc.
- **Resource provisioning:** The process of adjusting the amount and type of resources according to the changing demand and supply. Resource provisioning can be done proactively or reactively, based on historical data or real-time feedback, etc.
- **Task scheduling:** The process of determining the order and timing of executing tasks on resources to optimize certain objectives, such as completion time, energy consumption, cost, etc. Task scheduling can be done online or offline, based on priority or deadline, etc.
- **Workload balance:** The process of distributing the workload among the available resources to avoid overloading or underutilization. Workload balance can be achieved by using load balancing algorithms, such as round-robin, least connections, weighted round-robin, etc.

Funded by Horizon Europe Framework Programme of the European Union

BLOCKDIAGRAM

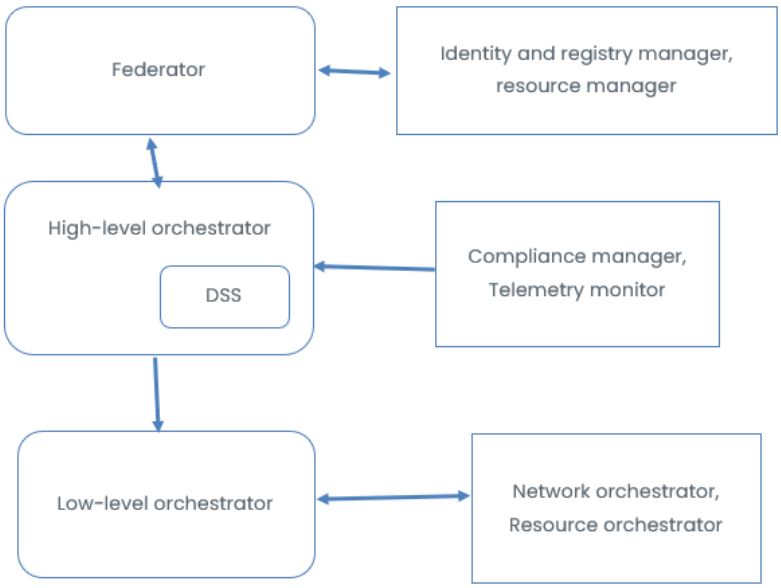
Simplified from feedback gathered about minimum functionalities:



- Management and scheduling module: managing all computational resources, including IoT devices.
- Allocation module: assigning resources for application execution.
- Discovery module: selecting the most suitable resource for any specific action.

Funded by Horizon Europe Framework Programme of the European Union

7. ORCHESTRATION



COMMON CAPABILITIES:

- **Federation**
  - Resource registry – as part of the work done within building block 1 (Security & Privacy)
  - Resource management – as part of the work done within building block 4 (Resource management)
  - Federator: taking care of the enablement of the most suitable spot for a specific deployment (linked with DSS developed within building block 8 – Artificial Intelligence). Shares information with the high-level orchestrator
- **Service description**
  - Decomposer: stores service description (linked with building block 3 – Data management for data storage/management). Information to be shared with DSS (building block 8 – Artificial Intelligence).
  - Both storage and the format on how the services must be described.
- **High-Level Orchestration**
  - Security guarantees must be undertaken - links with building block 1 – Security & Privacy. Also, security related to resources should be considered.
  - Data resources should also be addressed.
  - Meta-orchestrator: in charge of orchestrating and re-orchestrating (in case any event occurs – info coming directly from monitoring system (building block 7 – Monitoring & Observability) if it's something immediate or from the DSS (building block 8 – Artificial Intelligence) if the priority is lower). Sends this information to the low-level orchestrator which manages the deployment (building block 6 - Network). Shares information with

Funded by Horizon Europe Framework Programme of the European Union

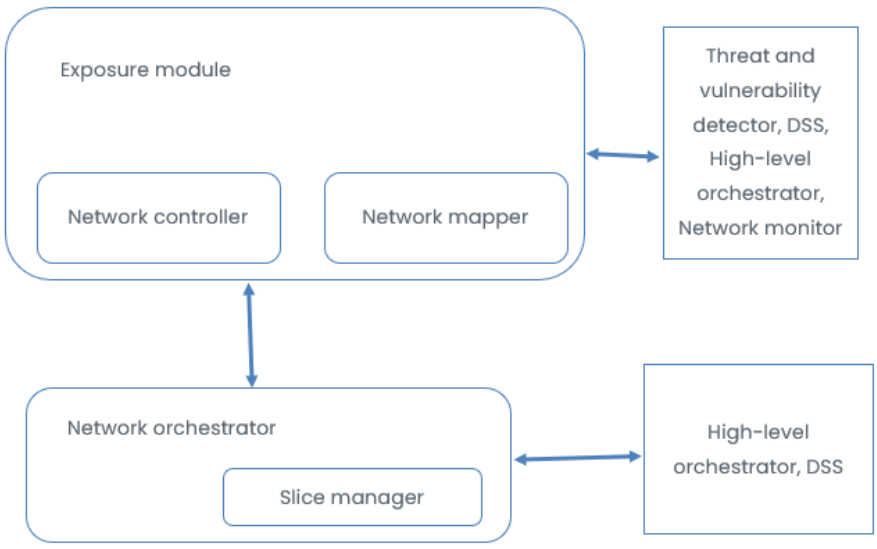
the federator in case there's the need of managing infra/resources for establishing a new cluster.

- **Low-Level Orchestration**
  - Include a composability necessary element called **"ADAPTER(s)"** that will make use of different interfaces to solve the complexity of underlying (needed connections). Example: edge node with very specific API to manage/handle.
  - Orchestrator: manages (and triggers) the deployment of an application, including autoscaling. Building block 6 (Network) enters into force if there is a requirement of initiating resources (such as NFV network slicing).

SPECIFIC FOR UCS

- FaaS Scheduling: Workflows of stateful functions (actors) generate asynchronous function calls as events which are routed within the same orchestration domain, or other orchestration domains, through a data plane where scheduling across multiple instances is based on weights/priorities.

8. NETWORK



COMMON CAPABILITIES:

- Exposure module: for network topology (to share information with the DSS for developing the deployment pattern)
  - Network controller: direct network topology data model
  - Alto protocol (network map): aggregator on top of the network controller
- Network orchestrator: orchestrate network resources (related to building block 5 – Orchestration)
  - Slice manager: provide slices under request to deploy applications.

Funded by Horizon Europe Framework Programme of the European Union

ADDITIONAL CONSIDERATIONS OF THE EXPOSURE MODULE:

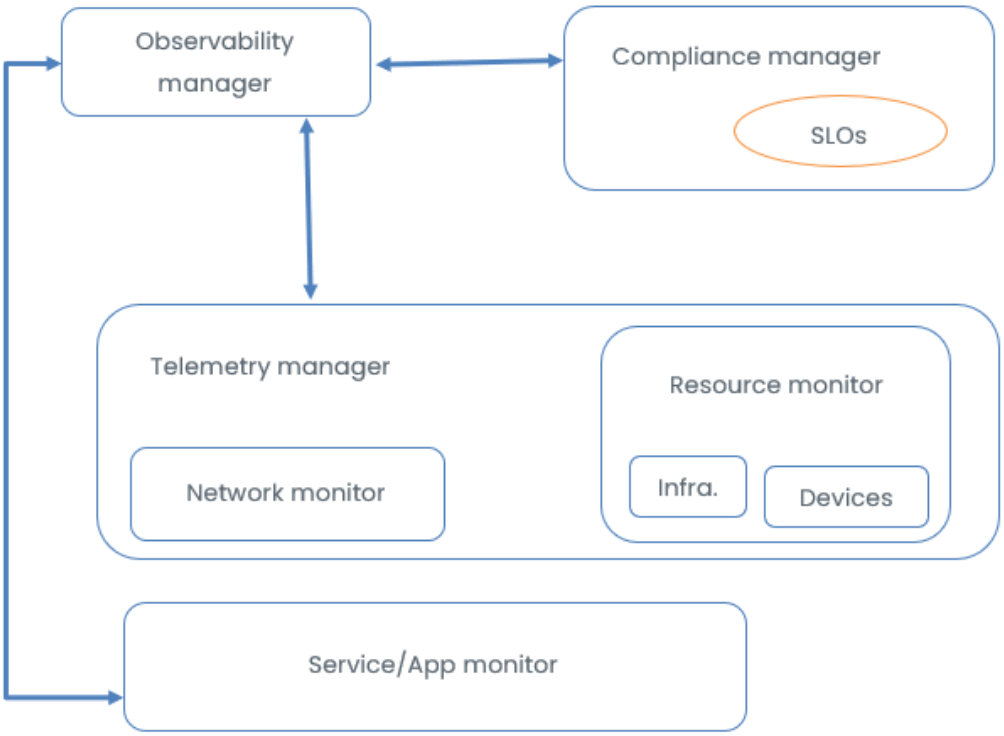
- Network management: manage network connectivity across all system components; receive monitoring data (coming from building block 7 – Monitoring & Observability) or security threats (from building block 1 – Security & Privacy) to perform corrective actions.
- Monitoring network data (from building block 7 – Monitoring & Observability): considered metrics: latency within the node, flow identification, CPU usage, battery charge, position of the node, RSSI of wireless links, network performance parameters (load and end-to-end latency), flow-level statistics
    - including in-network telemetry module: computing flow-level statistics directly in the data plane of network switches
- Network function acceleration: accelerating network functions (NAT, LB, Firewall, packet authentication, etc.) in host stacks (e.g., with eBPF), smartNICs and DPUs, and network switche

OPTIONAL (NOT MANDATORY) / ADDITIONAL COMPONENTS:

- Intelligent control plane (related to building block 8 – Artificial Intelligence): AI/ML for anomaly detection, network security (building block 1 – Security & Privacy), resource management
    - including swarm intelligence: leveraging switches and smartNICs for automating swarm operation with little interaction from control nodes: identification of nodes, swarm formation, isolation of traffic of different swarms

Funded by Horizon Europe Framework Programme of the European Union

9. MONITORING & OBSERVABILITY



COMMON CAPABILITIES:

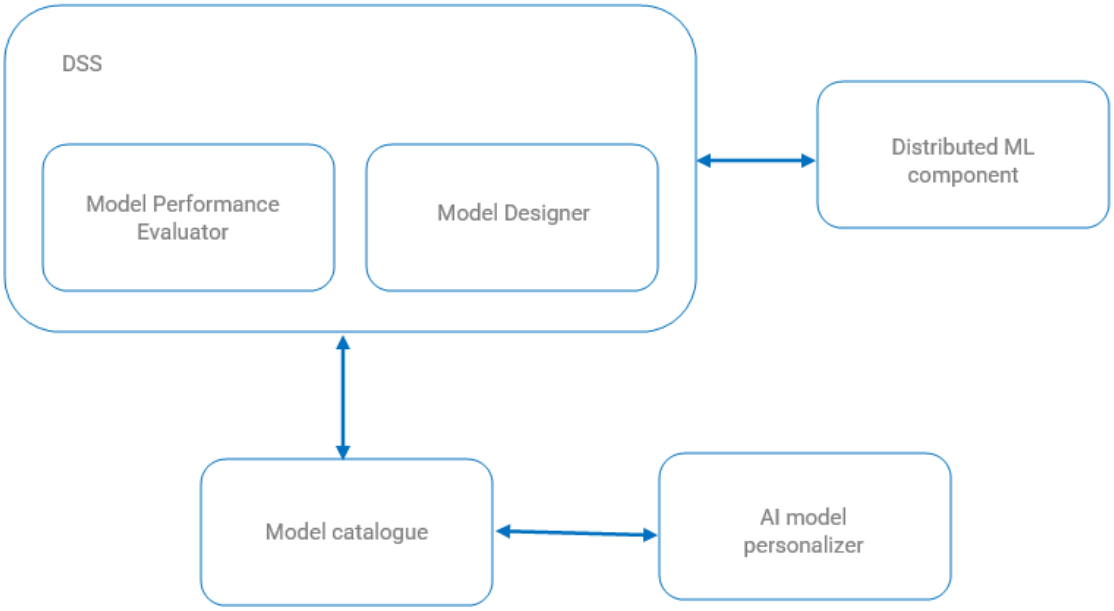
- Application monitoring module: monitoring the status of the application to identify underperformance issues not related to network or physical devices.
- Telemetry monitoring module: monitoring the connectivity status of the system to identify information loss.
- Infra monitoring module: monitoring the status of the infrastructure (mainly related to computing boxes or servers, those physical devices with high processing capabilities).
- Resource monitoring module(s): monitoring physical devices (mainly IoT ones).
- QoS/QoE module: containing metrics thresholds, established by default or further negotiated with the user and/or provider.
- Smart Observability module: gathering feedback from the monitoring modules and comparing it with the information stored in the QoS/QoE module to identify and predict breaches that must be prevented according to a previous negotiation.

The previously identified components provide the minimum set of functionalities to act/react according to the system and application health based on the specified params.
In case negotiation is out of the functionalities of this building block, it must receive these inputs from the building block in charge of it.

Funded by Horizon Europe Framework Programme of the European Union

Major outputs rely on notifications about potential QoS/QoE breaches during the execution of an application or system malfunctioning (e.g., low device battery) as a recommendation for a better deployment pattern.

10. ARTIFICIAL INTELLIGENCE



COMMON CAPABILITIES:

- Decision Support System: providing recommendations for deployment patterns and resource orchestration (ad-hoc spots) + AI orchestration recommendations. It also includes mapping functionalities.
    - Model performance evaluator + optimizations: to readapt the pattern to changeable conditions
    - Model designer: to develop the most suitable pattern adapted to each specific case
    - Model catalogue: model instances storage

OPTIONAL (NOT MANDATORY) / ADDITIONAL COMPONENTS:

- Distributed ML component: for managing the lifecycle of AI/ML models in distributed environments.
- AI model personalizer: allowing users to adapt existing models to their specific needs, including combining 2 or more, without the need to develop a new model

Funded by Horizon Europe Framework Programme of the European Union

11. CONCLUSION AND NEXT STEPS

As already presented in the previous documents of the series, there are three major steps to develop a reference architecture:

1. Define a common terminology to ensure all relevant stakeholders understand and use the same terms while referring to specific concepts.
2. Identify the common building blocks and the minimum set of functionalities to provide a simplified and easily understandable version of the architecture.
3. Design a reference architecture covering all aspects of the continuum.

This document focuses on the graphical representation of the Reference Architecture and the foreseen modules that provides the minimum set of functionalities to make it usable, and reusable. As already demonstrated by the projects contributing to its definition, additional functionalities can be added in order to address specific project needs.
Additionally, there is a set of documents that complement the work performed available at the EUCEI website:

- Position paper: it includes an analysis of the state of the art of existing reference architectures, identifying gaps and justifying the need of a homogenized one for the continuum. It also provides an overview of different solution architectures, mapped with the reference one, highlighting potential implementations of the presented architecture based on specific requirements.
- **Glossary:** list of terms and definitions as a common language for the continuum.
- **Taxonomy:** ontology containing the identified pillars and concepts.
- **Research challenges:** Technology gaps identified that will set the basis for future research.
- **Landscape:** graphical view of already implemented components that provides the functionalities previously identified.
- **Analysis of research results:** reusable methodology providing recommendations to improve the impact of project results.
- **Gap analysis:** list of missing implementations to provide all the functionalities needed to develop the whole system.

12. ABOUT EUCLOUDEDGEIOT INITIATIVE

The **EUCloudEdgeIoT.eu** initiative aims to realise a pathway for the understanding and development of the Cloud, Edge and IoT (CEI) Continuum by promoting cooperation between a wide range of research projects, developers and suppliers, business users and potential adopters of this new technological paradigm.
The EUCloudEdgeIoT initiative acts as an enabling force, to reach key outcomes:

- Support the definition of the large-scale pilots envisaged by the European Commission in line with the EU Data Strategy.

Funded by Horizon Europe Framework Programme of the European Union

- Baseline common open architecture for computing continuum research projects.
- Reinforce the collaboration between European public and private initiatives from cloud to edge to IoT.
- Increase the awareness of the importance of open source and standards for EU digital autonomy.

Within this initiative, TF3 Architecture main goals are as follows:

- Enable the architectural discussions among projects in the area of IoT/Edge and Cloud to create a continuum.
- Identification of the thematic areas and building blocks.
- Understanding the contribution of each project to the thematic areas, allowing the identification of cross-project synergies.

Funded by Horizon Europe Framework Programme of the European Union

EUCloudEdgeIoT.eu
Open Continuum

www.eucloudedgeiot.eu

@EU_CloudEdgeIoT

eucloudedgeiot

Grant Agreement No.: 101070030 **Topic:** HORIZON-CL4-2021-DATA-01-07
Call: HORIZON-CL4-2021-DATA-01 **Type of action:** HORIZON-CSA