

Component description

Objective of the component:

- IoTGateway:** Get a centralized entry point to the private container and services network in the Fractal platform
- Container security:** Make sure that all the software components run safely and securely, in secure runtime environments that communicate securely.
- Node monitoring:** Getting performance and status metrics to monitor the node health and process status

Fractal Features associated:

- IoTGateway:**
FRACTALITY --> COMMUNICATION --> DATA PROTOCOL --> MQTT
- Container security:**
SECURITY --> CERTIFICATE MANAGEMENT
FRACTALITY --> ORCHESTRATION --> SERVICES
ADAPTABILITY --> SERVICES ORCHESTRATION -> SCHEDULING
SECURITY --> PROCESS ISOLATION
- Node monitoring and system status:**
SECURITY --> MONITORING
SECURITY --> AUTHENTICATION, AUTHORIZATION

Inputs/Outputs:

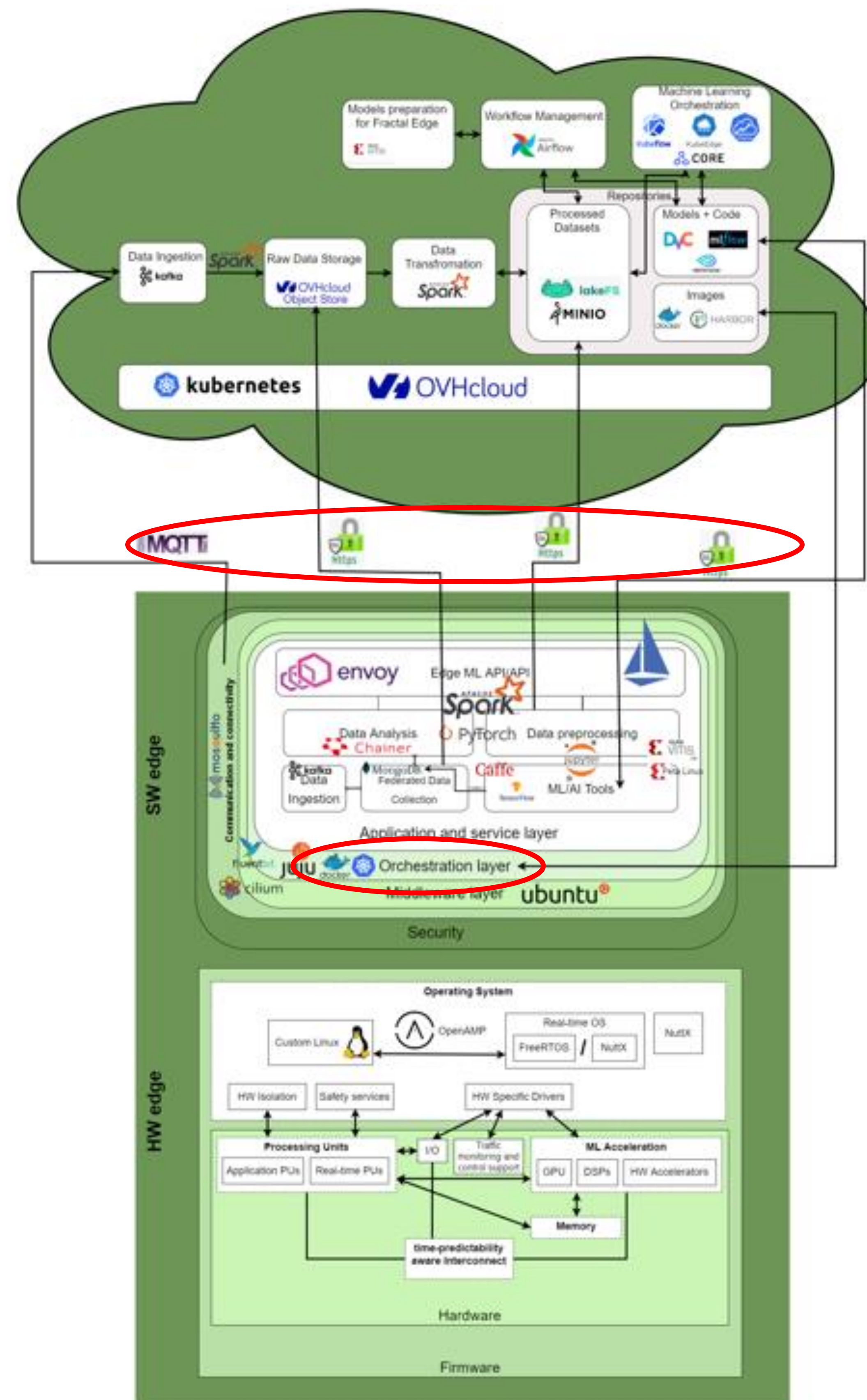
- IoTGateway:** Manages routes and redirects them to the specific services in the Fractal Platform. Gets HTTP(s) requests as input and sends back as output the service responses.
- Container security and Node monitoring and system status: ***

Integration:

- IoTGateway:** Apache APISIX can be integrated in Kubernetes clusters with the APISIX Ingress Controller to create Ingress K8S instances
- Container security and Node monitoring and system status: ***

* These are passive components that enhance security and do not directly interact or integrate with other components.

Component location



Images/Diagrams to describe the component and its processes

Get started

<https://apisix.apache.org/docs/ingress-controller/getting-started>

