



RAINBOW NEWSLETTER

ISSUE 5, OCTOBER 2021

RAINBOW is a Research and Innovation Action funder under the EU Horizon 2020 framework programme, focusing on producing an open, trusted **fog computing platform** facilitating the deployment, orchestration and management of scalable, heterogeneous and secure IoT services and cross-cloud apps.

RAINBOW FOG COMPUTING PLATFORM

RAINBOW enables IoT service operators to focus on their **services business logic**, delegating to RAINBOW's components the burden of **how and where services must be placed** in the fog continuum, establishing **secure collaboration** among entities and dealing with low-level aspects in data analysis including **heterogeneous resource management, mobility** and **data movement**. Towards this goal, RAINBOW's fog computing platform integrates all of the various modules and software subsystems developed during the project:

- Logically Centralized Orchestrator Backend
- Orchestration Lifecycle Manager
- Pre-deployment Constraint Solver
- Service Graph Editor & Analytics Editor
- Mesh Routing Protocol Stack
- Multi-domain sidecar proxy
- Resource & Application-level Monitoring
- Policy Editor
- Data Storage & Sharing
- Analytics Service
- Security Enablers



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871403

PROJECT INFORMATION

TITLE: RAINBOW - *A fog platform for secured IoT services*
GRANT AGREEMENT NO: 871403
CALL ID: ICT-15-2019-2020
CALL TOPIC: Cloud Computing
START DATE: January 1st, 2020
END DATE: December 31st, 2022
COORDINATOR: UBITECH
Ubiquitous Solutions

Follow us in social media:



Look for our hashtags!

#RAINBOW_H2020
#FogComputing #Industry40
#EdgeComputing #secureIoT



<https://rainbow-h2020.eu>



RAINBOW EARLY RELEASE

RAINBOW recently reached a major milestone by delivering the early release of its fog computing platform in July 2021. This first version abstracted and seamlessly handled the following important aspects:

Drag 'n' drop deployment description of IoT services

RAINBOW offers a User Interface that enables the end users to onboard their applications as also to manage their whole lifecycle. This is achieved by providing a collection of editors that enable the users to onboard their services following a guided form, graphically interconnect the services in order to formulate their applications templates and last but not least a graphical representation of their finalized application template from which they can proceed with the deployment of it and possibly provide any further descriptions for each individual deployment. The additional descriptions can be either modification of the services (envs, ports, devices, flavor, etc.) or addition of pre-deployment SLOs that will eventually materialize to Policies and Pre-deployment constraints. Of course, the descriptions can be further modified after the deployment of the application during runtime and materialize to runtime policies and constraints.

Near-optimal placement of IoT services on provisioned fog resources

Based on the Service Graph, the RAINBOW orchestrator creates Kubernetes-native deployments. The resulting pods (i.e., service instances) are placed on the fog infrastructure by the RAINBOW scheduler. In its final version, this scheduler will ensure that not only the resource requirements are fulfilled, but also the network Quality of Service (QoS) and trust requirements. For example, services that require a high bandwidth and low latency for communication among them, will be placed on fog nodes that fulfil these preconditions. Thus, instead of just evaluating the properties of each node in isolation, the RAINBOW scheduler additionally considers QoS properties for the entire communication paths between the nodes, resulting in a near-optimal placement of the scheduled services.



Network administration supporting encrypted IPv6 and reactive routing

RAINBOW targets deployments on Fog/Edge nodes that in most cases are wireless. For that reason, RAINBOW offers an encrypted IPv6 peer-to-peer network that uses cryptographic keys in order to authenticate and allow new nodes to be part of the network, as also Distributed Hash Table for the reactive routing and the dynamic load balancing. Through the above, we enable the platform to administrate the network as of which node can be part of the network and in situations that a node has been compromised or is not considered trusted, the platform can cut it off the network by making its key invalid and removing it from the routing table.

Establishment of trust across the device-fog-cloud stack

RAINBOW ensures security and privacy primitives across the device-fog-cloud-application stack by its trust and remote attestation mechanisms, including the provision of a secure "zero-touch configuration" overlay mesh network and runtime integrity verification of security-critical software components.

Pushing "intelligence" to the network edge

RAINBOW's Data Management services contribute to the enablement of interoperable and location-aware data processing across the fog continuum. This is achieved by pushing "intelligence" to the network "edge" with in-place data management and fog service analytics through decentralized edge APIs capable of "talking" to each other without the need for offline, manual, or human intervention. Specifically, RAINBOW's Distributed Data Storage and Sharing layer is realized on top of Apache Ignite, encapsulating novel algorithms for replication, sharing, indexing, and partitioning of Fog and IoT monitoring data. In addition, a high-level query model with operators for streaming analytics and optimized job compilation for fog deployments are introduced to abstract the complexity of streaming queries implementation. Finally, the RAINBOW data processing execution layer utilizes Apache Storm and extends it with novel scheduling algorithms, which optimize operator placement, data transfer, and overall query execution time.

RAINBOW SUPPORTED EVENTS

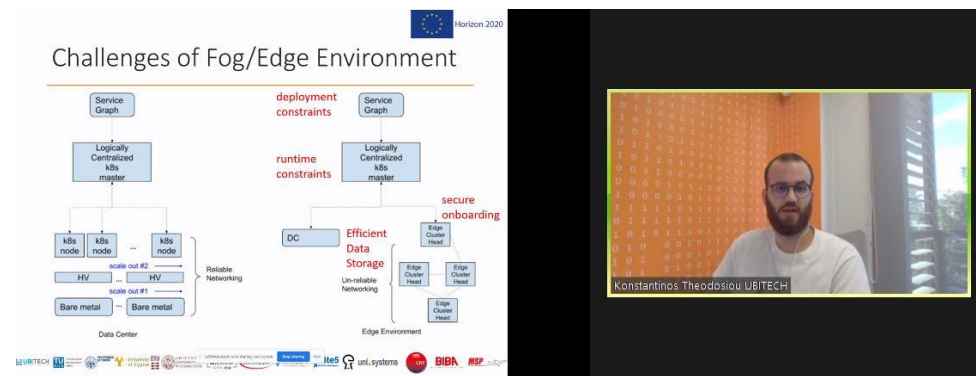
16th International Conference on Availability, Reliability and Security (ARES 2021)

The ARES 2021 conference took place virtually, from 17th to 20th of August. During the conference, RAINBOW's partners **Infineon Technologies** presented the key management for a fog architecture in the context of the RAINBOW platform and showed how the computations of a recently published proof-of-concept implementation of Direct Anonymous Attestation can be distributed in this specific fog environment. Moreover, they provided details on an embedded system-level implementation and performance benchmarks for IoT applications keys stored with proper hardware-based protection within a Trusted Platform Module. Read more at: <https://dl.acm.org/doi/10.1145/3465481.3470063>

Unleashing the Potential of Cloud, Fog, and Edge Computing in Europe

On 29th of September 2021, under **H-CLOUD's Technical Community Event**, the **RAINBOW** and **PLEDGER H2020** projects presented some of their latest technical outcomes. During the event, RAINBOW members from **UBITECH** and **University of Cyprus** demonstrated the advanced features included in the first release of RAINBOW's fog computing platform and provided an inside view on RAINBOW's approach for pushing "intelligence" to the network edge with in-place data management and fog analytics services.

Additional information: <https://www.h-cloud.eu/event/h-cloud-technical-community-event-unleashing-the-potential-of-cloud-fog-and-edge-computing-in-europe/>

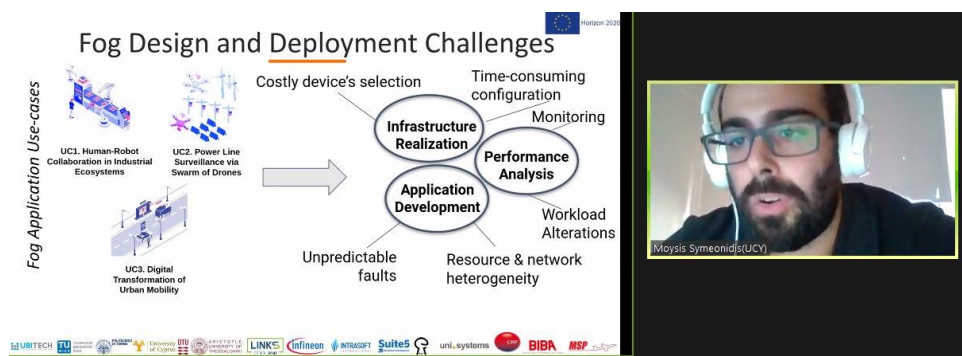


Challenges of Fog/Edge Environment

The slide compares two architectures:

- Data Center:** A Service Graph connects to a Logically Centralized k8s master, which manages multiple k8s nodes. These nodes are connected to a High Voltage (HV) network, which in turn connects to Bare metal infrastructure. This setup is labeled as 'Reliable Networking'.
- Edge Environment:** A Service Graph connects to a Logically Centralized k8s master. This master is connected to a DC (Data Center) and an Efficient Data Storage. The Edge Environment consists of Unreliable Networking connecting to multiple Edge Cluster Heads and Edge Cloud Heads. This setup is labeled as 'secure onboarding'.

Additional labels include 'deployment constraints' and 'runtime constraints' between the two architectures.



Fog Design and Deployment Challenges

The slide illustrates the challenges in fog computing:

- Fog Application Use-cases:** Includes UC1. Human-Robot Collaboration in Industrial Ecosystems, UC2. Power Line Surveillance via Swarm of Drones, and UC3. Digital Transformation of Urban Mobility.
- Challenges:**
 - Costly device's selection
 - Time-consuming configuration
 - Monitoring
 - Performance Analysis
 - Workload Alterations
 - Resource & network heterogeneity
 - Unpredictable faults
- Core Processes:** Infrastructure Realization and Application Development.



THE RAINBOW APPROACH VIDEO

The first RAINBOW VIDEO is OUT! RAINBOW's consortium released the first video of the project, one that aims to awaken the public about the prospects of RAINBOW.



Our video, entitled "*RAINBOW Approach*", is the first of a series of videos which will introduce and explain all of the project's aspects to the audience. This initial production provides a general introduction, regarding the concept and the targets of the project. More specifically, it presents critical points regarding the RAINBOW project such as:

- The philosophy behind RAINBOW's platform
- The vision of RAINBOW project
- What does RAINBOW offer?
- What are the benefits of the RAINBOW solution?
- In which technological areas RAINBOW will be demonstrated?

The "RAINBOW Approach" video is available through RAINBOW's YouTube channel and can be found here: <https://www.youtube.com/watch?v=f-1ZDvh8Y0w>



@RainbowProjectH2020



@RainbowH2020



rainbow-project-h2020



rainbow.2020.eu



/channel/UCRcOGrIN
aV9wWh6Bih11-KA



Visit our website and subscribe to our newsletter to receive it in your email!

<https://rainbow-h2020.eu/contact-us/>