# SEcure & DistribUted intelligence for Constrained Environments - Are you yet SEDUCEd?

15 June 2021, 02:00

Anna Hristoskova
Nicolás González-Deleito

*Recent developments in distributed AI on the edge result in new approaches to secure & targeted distributed analytics. Within Sirris, in the scope of several research projects, we are exploring energy- and resource-efficient scaling of AI-based applications among the existing edge infrastructure, while preserving privacy-sensitive data.*

With the advent of edge nodes with increased computational and storage capabilities, companies leverage on these by performing a large range of increasingly resource-demanding applications through a growing number of highly instrumented devices. In the case of industrial monitoring and control applications for example this results in massive amounts of data, distributed across a multitude of devices in the field. Currently, all these data are typically transferred to a central location (e.g. cloud) in view of exploitation by intelligent machine learning and AI.

## Limitations of centralised cloud computing

However, this traditional model of centrally creating and analysing large data collections is not a viable solution for targeted distributed analytics. Offloading processing capabilities to the cloud requires dealing with the following limitations and constraints:

> **availability** of the underlying communication channels and of the cloud infrastructure

> necessary mechanisms to **secure data** in transit and at rest (esp. when **privacy-sensitive** data is considered)

> **costs** incurred from the transmission of data and by the usage of the backend cloud infrastructure

> **unacceptable latency** of the underlying communication channels for many industrial control application and applications with real-time constraints

Furthermore, depending on the application and underlying infrastructure only a **fraction of the data** is transferred to the backend for analytics due to bandwidth limitations or cost constraints, while the remaining data is discarded at a very early stage.

## Edge computing

An alternative to the traditional model, which brings the data to the intelligent algorithms, is to bring these algorithms to the data, while still leveraging the information from many users: distributed AI on the edge.

Edge computing has the potential to reduce the volume of data that must be moved and to reduce overall traffic thanks to **massively parallel and distributed architectures**. It shortens the distance that data must travel thus decreasing communication latency and transmission costs. The distribution of computational-intensive tasks to local resources increases the scalability and leads to considerable improvements in response times for real-time critical applications. Further, the centralised instance is no longer a single point of failure, but the devices can work independently for a while.

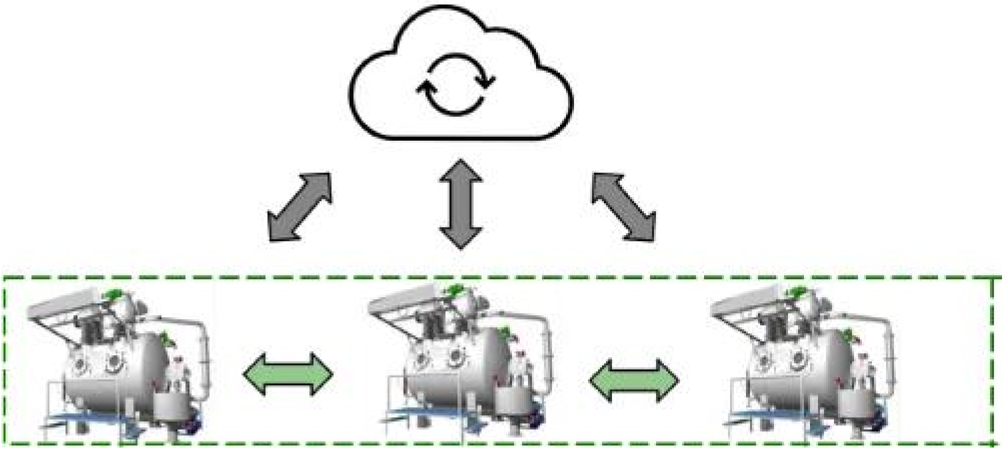
## Secure & Distributed Intelligence in the scope of 3 European projects

Within Sirris, we are exploring within the 3 European R&D project listed below energy- and resource-efficient approaches to scaling AI-based edge computing applications through their orchestration and distribution among the existing edge infrastructure, while preserving the users' privacy. Distributed and composable ML models and techniques that scale horizontally among edge devices (as well as vertically to the cloud) are also the basis for the applications to guarantee high-quality decision making.

This will empower edge computing to provide real-time processing and analytics capabilities near the point of use and source of data. It will significantly reduce the need for the expensive and relatively slow connection to the cloud as a bottleneck to analysis, while no personal information is stored in a centralised location. Data collection, ML and inference tasks of AI applications can be distributed in a federated architecture. Such a solution is robust because tasks can migrate in case of component failures.

**DAIS** (ECSEL, May 2021 - April 2024) - aims to research and deliver distributed artificial intelligent systems by solving the problems of running existing algorithms on vastly distributed edge devices. The research and innovation actions in DAIS are organised around eight different supply chains. Five of these focus on delivering the hardware and software that is needed to run industrial-grade AI on different type of networking topologies. The remaining supply chains demonstrate how known AI challenges, from different functional areas, are met by this pan-European effort.
The Belgian use case, provided by Sentigrate, focuses on an on-the-edge **positioning** engine.

**MIRAI** (ITEA3, December 2020 - November 2023) - aims to develop the MIRAI Framework Building Blocks (MFBB), based on AI techniques, to enable smart and sustainable planning and operation of IoT and Edge computing applications. These will supplement the traditional scaling approach to the cloud with horizontal scaling of IoT and edge computing applications amongst edge devices.
The Belgian use cases, provided by 3E, Macq and Shayp, focus



**SunRISE** (PENTA, September 2019) - intends to develop a shared security solution to tackle: (i) ML on the edge facilitating IoT security analytics to defend against intrusion attacks and detect anomalies and misconfigurations, (ii) sharing relevant security data across different stakeholders and applying ML on the combined data and models, and (iii) evaluating homomorphic encryption as a privacy enhancing technology and applying ML on the combined encrypted datasets. The Belgian partners (Engie Laborelec, NXP and Sirris) will demonstrate the SunRISE results in the context of an **energy communities** (smart grid) use case.

In order to support these and future activities, the Sirris's Data and AI Competence Lab and Software Engineering group have joined forces combining knowhow on both distributed AI approaches for resource constrained devices and security & privacy of data (analytics) on the edge, fog, cloud and in transit.

]]>

## Authors

Anna Hristoskova

Nicolás González-Deleito