Supporting Privacy Preservation by Distributed and Federated Learning on the Edge

Research And Innovation 23 September 2021 Last Updated: 30 September 2021

by Davide Bacciu (UNIPI), Patrizio Dazzi (CNR-ISTI) and Alberto Gotta (CNR-ISTI)

The H2020 TEACHING project puts forward a human-centered vision for adapting and optimising autonomous applications, leveraging users' physiological, emotional and cognitive states. Such a goal can be achieved by building a distributed, embedded and federated learning system complemented by methods and tools to enforce its dependability, security, and privacy preservation.

Automation enables processes to run with minimum human involvement in the sensing, decision, and actuation loops. Automation can be used to operate cyber-physical systems of systems (CPSoS), comprising complex, multi-faceted, and dynamic virtual and physical resources that operate at the crossroads of the physical and virtual worlds. Humans interact with the autonomous system either as passive end-users (such as passengers in autonomous transportation) or as active co-operators in a mutual empowerment relationship towards a shared goal. Such a cooperative, connected, and autonomous system of systems can be a game-changer in multiple domains if it can positively exploit such an inescapable human factor.

The H2020 TEACHING project [L1] is a three-year endeavour supported by a consortium of 10 partners from five European countries (Austria, France, Germany, Greece, Italy) aiming to design an autonomous CPSoS application with a human-centric perspective, bringing in critical requirements in terms of adaptivity, dependability (safety, security, reliability) and privacy. The

project realises a computing and communication architecture with an integrated artificial intelligence (AI) as a service (AIaaS) platform supporting concepts of dependable engineering, federated, and distributed learning.

AI is central to the TEACHING perspective, as it is a crucial technology to develop autonomous applications – particularly when such applications are realised within the inherently dynamic, connected and interacting context of a CPSoS. An effective AI for the CPSoS should exhibit certain key design features. Machine intelligence, in such scenarios, is distributed and pervasive, where the AI components can be potentially deployed in every element of the CPSoS, enabling it to embed intelligence at the edge, close to where the information is produced by devices or close to where the application consumes the AI predictions. Information processing should follow as much as possible principles of locality and compositionality, respecting the inherently distributed nature of the system of systems. This allows us to contain the deluge of noisy, redundant, heterogeneous, and fast-flowing data produced by the CPSoS elements, thus minimising the negative impacts on communication, storage, and energy consumption. Local consumption of information can also be an advantage in unreliable connectivity scenarios and when data privacy is a crucial issue.

A human-centric perspective on CPSoS intelligence inevitably brings up how to elicit the necessary feedback to drive adaptation in the right direction. When the human is in the loop, it is natural to consider him/her a source of informative and dependable teaching information. TEACHING leverages such a human-centric perspective by developing novel adaptation mechanisms that exploit noisy learning signals under the form of human psycho-physiological reactions. Such concepts of weak supervision are integrated with aspects of lifelong learning [1], where the components of the learning federation are allowed to learn continuously from streams of experiences.

The principles of the locality of computation, previously highlighted for AI models, should also be consistently applied to the issue of dependability. The AI models cannot and should not be left alone at the edge of the CPSoS, especially in safety and mission-critical applications. They should be supported and followed at the edge by dependability and security-related watchdogs. This entails the need for novel systems and engineering methods, also developed within TEACHING, providing CPSoS with native support to cybersecurity and dependability requirements, possibly integrating AI and dependability aspects within the same edge devices.

The TEACHING project investigates the development of learning models explicitly designed to support key concepts of computational efficiency, processing of noisy streaming data, and federated learning. The learning methodology is being built around the concepts of randomised recurrent neural models from the Reservoir Computing paradigm [2]. These models

allow effective predictors to be realised that can be efficiently embedded on edge devices containing computational, memory, and energy fingerprints. They also ease the development of robust mechanisms to fuse the local AI models of the federation into a centralised model without needing to transfer data collected locally on edge devices [3]. This means that it is possible to realise a federated learning deployment with an excellent trade-off between accuracy and privacy preservation as data does not need to be communicated out of the edge devices where it is produced. The conceptual architecture of the TEACHING project is depicted in Figure 1. At its bottom stands a heterogeneous set of resources realising the CPSoS. The central part of the figure represents the salient aspects of the TEACHING ecosystem, which revolves around three main pillars.

1. The (distributed) computing and communication platform, organised accordingly with the principles of edge computing, aiming at the efficient management of the pool of resources belonging to the TEACHING CPSoS;
2. The mechanisms, the policies, and a set of design patterns developed ad-hoc to ensure the platform's security and privacy and to satisfy the requirements of dependability, making the platform a viable solution in real-world scenarios;
3. An AI-as-a-service subsystem supporting federated learning processes based on reservoir computing that enables continuous learning that exploits human feedback to improve its performance.

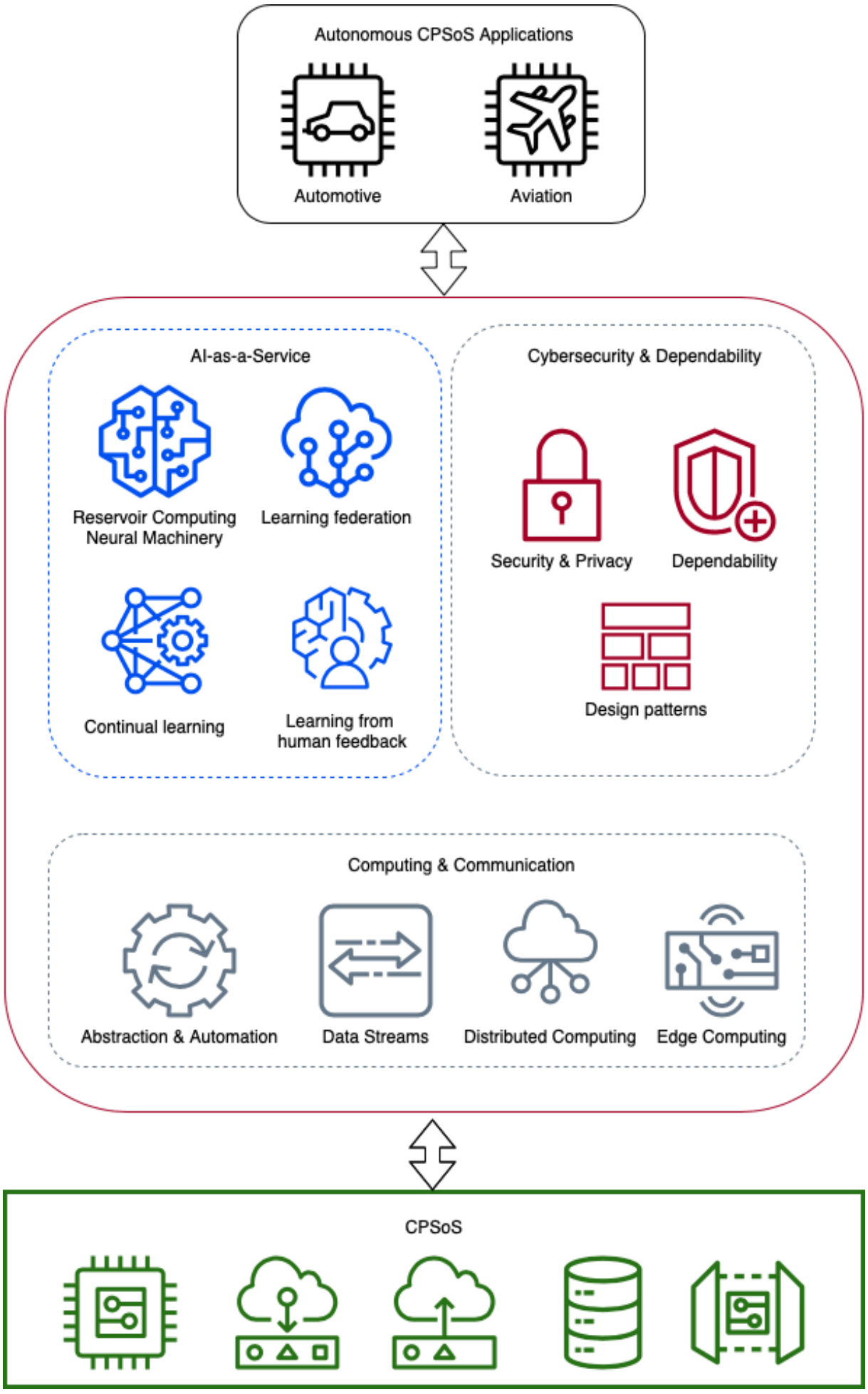
Autonomous CPSoS Applications
Automotive
Aviation
AI-as-a-Service
Reservoir Computing
Neural Machinery
Learning federation
Continual learning
Learning from
human feedback
Cybersecurity & Dependability
Security & Privacy
Dependability
Design patterns
Computing & Communication
Abstraction & Automation
Data Streams
Distributed Computing
Edge Computing
CPSoS

Figure 1: Conceptual architecture of TEACHING.

The upper part of the figure reports two use cases, in the fields of autonomous automotive and avionic transport, that demonstrate the added value of TEACHING. Such use cases are characterised by high challenges connected with their needs for autonomy, dependability, and capability to adapt to human needs and reactions. They are also highly relevant for the industrial competitiveness of the European Union, and they are hence excellent testing cases for the TEACHING design.

Link:
[L1] https://teaching-h2020.eu

References:
[1] G. L. Parisi, et al.: “Continual Lifelong Learning with Neural Networks: A Review”, Neural Networks, 113, 54-71, 2019.
[2] M. Lukoševičius, et al.:, “Reservoir computing trends”, KI-Künstliche Intelligenz, 26(4), 365-371, 2012.
[3] D. Bacciu, et al.: “Federated reservoir computing neural networks, “Proc. of the Int. Joint Conf.on Neural Networks (IJCNN 2021), IEEE, 2021.

Please contact:
Davide Bacciu, University of Pisa, Italy
davide.bacciu@unipi.it

Patrizio Dazzi, Alberto Gotta
ISTI-CNR, Italy
patrizio.dazzi@isti.cnr.it, alberto.gotta@isti.cnr.it