OASEES: An Innovative Scope for a DAO-Based Programmable Swarm Solution, for Decentralizing AI Applications Close to Data Generation Locations

Ioannis P. Chochliouros[1(✉)], Michail -Alexandros Kourtis[2], George Xilouris[2], Wouter Tavernier[3], Enrique Areizaga Sanchez[4], Margarita Anastassova[5], Christian Bolzmacher[5], Nikolay Tcholtchev[6], Antonello Corsi[7], Panagiotis Trakadas[8], Marta Millet[9], Christos Xenakis[10], Adnan Imeri[11], Francesco Bellesini[12], Paride D'Ostilio[13], Albertos Markakis[14], Ihsan Bal Engin[15], Antonis Litke[16], Lucrezia Maria Quarato[17], Diego Cugat[18], Georgios Gardikis[19], Charilaos Zarakovitis[20], Stephane Bouilland[21], Zaharias Zaharis[22], Christina Lessi[1], Dimitrios Arvanitozisis[1], and Anastasia S. Spiliopoulou[1]

[1] Hellenic Telecommunications Organization (OTE) S.A., 99 Kifissias Avenue, 15124 Maroussi-Athens, Greece
ichochliouros@oteresearch.gr
[2] National Center for Scientific Research "Demokritos", Athens, Greece
[3] IMEC—Department of Information Technology, Ghent University, Ghent, Belgium
[4] Fundacion Tecnalia Research & Innovation, Derio, Spain
[5] Commissariat à L'Energie Atomique et aux Energies Alternatives, Paris, France
[6] Fraunhofer Gesellschaft Zur Forderung der Angewandten Forschung EV, Munich, Germany
[7] Engineering – Ingegneria Informatica SpA, Rome, Italy
[8] National & Kapodistrian University of Athens, Athens, Greece
[9] Robotnik Automation SLL, Barcelona, Spain
[10] Inqbit Innovations Srl, Bucharest, Romania
[11] Infrachain SBL, Luxembourg, Luxembourg
[12] Emotion Srl, Le Galatina, Italy
[13] ASM Terni SpA, Terni, Italy
[14] Adrestia Erevnitiki Idiotiki Kefalaiouxiki Etaireia, Iraklio, Greece
[15] Senso Engineering BV, Groningen, The Netherlands
[16] Infili Technologies S.A., Athens, Greece
[17] SCM Group SpA, Rimini, Italy
[18] CapGemini Engineering, Barcelona, Spain
[19] Space Hellas S.A., Athens, Greece
[20] Axon Logic, Athens, Greece
[21] Fondation Hopale, Berck Sur Mer, France
[22] Aristotle University of Thessaloniki, Thessaloniki, Greece

Abstract. As traditional linear models have proved to be ineffective in perspective of the stagnant decision-making and inefficient data federation, the pathway onwards a European data sovereignty dictates for a sustainable and circular economy across diverse market sectors. In this scope, the EU-funded OASEES project

© IFIP International Federation for Information Processing 2023
Published by Springer Nature Switzerland AG 2023
I. Maglogiannis et al. (Eds.): AIAI 2023 Workshops, IFIP AICT 677, pp. 91–105, 2023.
https://doi.org/10.1007/978-3-031-34171-7_7

has identified the need for a novel, inclusive and disruptive approach regarding the cloud to edge continuum and swarm programmability and also supporting multi-tenant, interoperable, secure and trustworthy deployments. In the present paper we discuss actual challenges for the management and orchestration of edge infrastructure and services to exploit the potential of edge processing. Then we discuss the concept and fundamental features of the OASEES approach together with technology challenges that are to be covered by the intended system development. We also discuss, in brief, a set of several vertical edge applications with significant market impact.

Keywords: 5G · AI · blockchain · cloud hosting · compute continuum · DAO · decentralized applications · edge computing · edge processing · edge sharing · enhanced platform awareness · ML · MLOps · swarm computing · secure edge

1 Introduction

The huge increase in device connectivity and produced data has resulted in the extended growth of diverse intelligent processing services to create insights and exploit data in a multi-modal manner. At present, the most powerful data processing – as it is observed in various systems – takes place in a centralized way at the cloud and this offers the opportunity and the capability not only to scale but also to allocate involved and available resources both on demand and efficiently. Centralized data processing [1] actually occurs when all data is collected to a single centralized storage area and processed upon completion by a single computer with often very large architectures in terms of memory, processor and storage. All of the data is saved/stored in a centralized data storage system. Protection level decisions and authorised access are the responsibility of the respective system administrator. In this context, centralized processing can so offer several distinct benefits for the involved "actors" as, among others: it helps in reducing the cost as there is no emphasis on more hardware and machines to be involved; it can provide more enhanced data security, and; the data and the program on each information system are independent to other information systems, thus extending security and trust. Cloud hosting [2] makes applications and websites accessible by using dedicated cloud resources. Unlike traditional hosting processes, the respective solutions are not deployed on a single server; instead, a network of connected virtual and physical cloud servers does host the application – or the website – ensuring greater elasticity and scalability. "Key features" of this context may implicate for: (i) applications and solutions being deployed on a cloud network rather than an on-premises, single server; (ii) resources can be scalable to user needs; (iii) involved entities/organizations only pay for the resources they use, and; (iv) solutions are automated and controlled using Application Programming Interfaces (APIs), web portals and mobile applications. This also offers flexibility and reliability: for the former, as traditional hosting services offer limited bandwidth, cloud hosting scales to accommodate traffic spikes or seasonal demands; for the latter, hardware failures do not cause downtime because sites and applications are hosted on a network of server; thus, traffic travels across separate network interfaces, where it is segregated and secured.

However, centralized processing and cloud hosting although they have been widely used and deployed in numerous systems, bound – and up to a certain extent "limit" – their services and/or applications to operate in a resource restricted manner, relying most of times on large single entities to offer: (i) authentication; (ii) data storage; (iii) data processing; (iv) connectivity, and; (v) vendor-locked environments for development and orchestration. This significantly limits the users from their data governance and even identity management [3, 4], as it prevents them from efficiently managing their identities and access, restricts their visibility into identities and access privileges and does not help them to implement any of the necessary controls for preventing potential inappropriate or risky access. Data governance implicates for the sum of policies, processes, standards, metrics, and roles being able to ensure that data is used effectively to help an entity to realize its objectives. Data governance establishes the responsibilities and processes which ensure that the data being used is not only of high quality but is also secure. As such, it defines who takes what actions, on what data, in which situations and what methods are in use. On the other hand, an identity management (IdM) system prevents unauthorized access to systems and resources, helps prevent exfiltration of protected data and raises alerts and alarms when access attempts are made by unauthorized users or programs, whether from inside or outside the entity's perimeter. IdM includes polices and technologies to properly identify, authenticate and authorize people, groups of people, or software applications through attributes (including user access rights and restrictions based on their identities). Similarly, existing solutions for edge device authentication [5–7] require a centralized entity to trust them and authenticate them, rendering a non-portable identification paradigm.

2 Challenges for a More Efficient Edge Processing

Over the past years and following the fast progress of the underlying IT and network infrastructures (especially within the "5G and beyond" context), several platforms and/or related solutions, also including open-source- based ones, have been emerged focusing primarily on the management and orchestration of edge infrastructure and services [8–11]. However, in order to fully exploit the potential of edge processing [12], a need has been raised towards proposing for a "more holistic solution" by embracing the entire compute continuum [13] (the compute continuum allows the exploitation of hybrid IoT-Edge-Cloud infrastructures with great flexibility while guaranteeing high-performance) as well as by including central infrastructures (public clouds and networks) and smart devices. In fact, edge processing occurs when the computation of data is carried out directly in the smart sensor node or at the gateway of the network, intending to save power consumption and ensure that data is kept confidential, thus allowing involved "actors" to analyze critical information at the node level and reduce anomaly detection time(s). The idea is to "put" basic computation as close as possible to the physical system, making the involved IoT (Internet of Things) device as "smart" as possible. In this context edge processing can implicate for several benefits such as: (i) confidentiality, as data is not sent to the cloud and is locally stored on the device or the other equipment used; (ii) cost reduction, as latency and throughput of high-volume time-series asset data can be optimized - in fact, reducing the amount of useless machine data sent and stored in

the cloud leads to significant benefits as it enables real-time distributed applications and simultaneously eliminates the need for complex systems; (iii) lower latency, implicating that a minimal delay in the repair of equipment is essential for assets which are assessed as mission-critical.

Under the previously discussed framework and with the purpose of meeting performance, cost and/or potential legal requirements, cloud resources are nowadays moving toward the edge of the network to "bridge the gap" between resource-constrained devices and distant but powerful cloud Data Centres (DCs). Edge computing [14, 15] is an emerging computing paradigm which refers to a range of networks and devices at or near the user. Edge (which implicates for both edge devices and the network edge) is about processing data closer to where data is being generated, enabling processing at greater speeds and volumes, leading to greater action-led results and experiences in real time. The wide adoption of the recently coined fog and edge computing paradigms alongside conventional cloud computing creates a novel scenario, known as the "cloud continuum" [16], where services may benefit from the overall set of resources to optimize their execution. To operate successfully, such a cloud continuum scenario demands for novel management strategies, enabling a coordinated and efficient management of the entire set of resources, from the edge up to the cloud, designed in particular to address key edge characteristics, such as mobility, heterogeneity and volatility. While recent studies propose that the future of cloud computing [17] will be distributed and heterogeneous [18], there is a lack of open management frameworks to address this sort of dispersion and heterogeneity. Commercial solutions for hybrid core/edge management, such as Azure Edge Stack [19] indeed exist, but these are usually "closed", restricted to specific deployment scenarios and only provided as managed services (i.e., not suitable for private (fully on-premises) deployments).

Another essential "gap" to deal with is related to the ease of access from the point of view of the data scientists and engineers. Public clouds already provide user-friendly abstractions (notebooks, simplified administration interfaces, graphical workflow designers, etc.) to data experts, so that the latter can concentrate on the management of the data and the selection and optimization of the ML (Machine Learning) / AI (Artificial Intelligence) algorithms, rather than on the management of the physical and virtual resources which are needed and committed. This is actually a feature missing from existing edge orchestration solutions [20]. Edge orchestration [21–23] is a term that describes the use of an "Edge Orchestrator" to manage, automate and coordinate the flow of resources between multiple types of devices, infrastructure and network domains at the edge of a network. Edge orchestration allows businesses and organizations to efficiently route data resources so that to avoid potential bottlenecks, reduce latency and scale their network as needed, per case. The goal of edge orchestration in a network is about establishing more intelligence to the network in which real-time network events, traffic or other dynamic requests can be handled automatically, at the edge of the network. This eases the effective deployment of resources and allows near-instantaneous provisioning of network services. It can also help reallocation of network resources across multiple devices or other sort of equipment used.

Furthermore, security is a similarly important aspect [24, 25] as edge infrastructures can be highly dynamic, involving ad-hoc onboarding of edge nodes and smart devices,

possibly under different status of ownership (e.g., in multi-actor environments). In such a volatile context, in order to guarantee data privacy and availability (here data availability means that information shall be accessible to authorized users) there is a need to continuously verify the integrity of both infrastructure and services across the considered compute continuum [26].

3 "OASEES" Concept: Features and Technology Challenges

Following to the various challenges and trends discussed in the previous section, the ongoing OASEES [27] project aims to deliver and promote a European, fully open-source, decentralized and secure Swarm programmability framework for edge devices and leveraging various AI/ML accelerators (Field Programmable Gate Arrays [28] (FPGAs), Spiking Neural Networks [29] (SNNs), Quantum [30]), while supporting a privacy preserving Object ID federation process [31]. More specifically, OASEES will be built leveraging existing open-source edge orchestration solutions and intends to be capable of:

- *Managing the lifecycle of services across the compute continuum* [32, 33] by orchestrating heterogeneous resources in the cloud, WAN (Wide Area Network), edge and smart device domains. Resources from Central Processing Units (CPUs), Graphics Processing Units (GPUs), NPUs, FPGAs bespoke chips (e.g., for Spiking Neural Networks [34] acceleration) and Quantum processors [35] are to be pooled and jointly managed to optimize ML at the edge, for maximum performance and energy efficiency. While the focus is expected to be on managing the edge and smart device domains, adaptors to popular public clouds will also be integrated, for supporting end-to-end (E2E) services with the appropriate Quality of Service (QoS) guarantees at WAN network level (i.e., core- edge interconnect).
- *Promoting the development of decentralized ML/AI edge services* [36] by means of an SDK (Software Development Kit) and in the form of Decentralized Applications [37] (DApps) in a user-friendly notebook-style abstractions for data scientists and engineers. DApps can operate autonomously, typically through the use of smart contracts, that run on a decentralized computing, blockchain or other distributed ledger system. The "serverless" fashion for Swarm deployment will make use of distributed ML platform capabilities and a Distributed Data Fabric; this will essentially realise the vision of Decentralized Artificial Intelligence as-a-Service [38] (DAIaaS), an essential component towards a smarter Internet of Everything (IoE). DAI is a model that allows for the isolation of processing without the downside of aggregate knowledge sharing. By virtue, it enables the user to process information independently, among varying computing apparatuses or devices. In doing so, one can achieve different results and then analyze the knowledge, creating new solutions to a problem which a centralized AI system would not be able to.
- *Supporting multi-actor/multi-domain deployments*, by: (i) enforcing security and trustworthiness; (ii) enabling the federation with peer OS instances [39] in other administrative domains (multi-domain operation) and; (iii) fostering monetization by advertising/trading capabilities and resources in third-party Marketplaces (including

the Marketplace of the European Open Science Cloud (EOSC) [40]; EOSC's ambition is to provide European researchers, innovators, companies and citizens with a federated and open multi-disciplinary environment where they can publish, find and re-use data, tools and services for research, innovation and educational purposes).

OASEES has identified specific research topics and corresponding challenges which it aims to directly "address" as briefly discussed in the following sections:

***Programmable Frameworks for Swarm and Edge Computing*:** The existing management and orchestration frameworks landscape [41] is scattered in systems focusing either on cloud management, NFV MANO [42] (Network Functions Virtualization Management and Orchestration), Software Defined Networking- (SDN) based network control [43] or IoT-focused edge platforms [44]. OASEES' aim is to reconcile and "go beyond" existing control systems and APIs into an open programmable Swarm framework so that to enable an IoT-to-edge-to-cloud continuum where services can be developed, benefiting from: (i) an IoT-to-edge-to-cloud infrastructure model enabling to characterize a wide variety of related resources, building further on existing State-of-the-Art (SotA) such as OCCI [45]; (ii) a de/composable service model based on SotA such as TOSCA [46] enabling to characterize which components require performance profiling and/or allow hardware acceleration, which components require security measures (monitoring, anomaly detection, etc.), or what particular reliability or QoS-based control loops. Composability in the service model of OASEES also means that services can recursively build upon each other – this will enable one service to serve as an intelligence or data-processing component for another; (iii) a security- and intelligence-aware SDK enabling lifecycle management and asymptotic orchestration of data rich services. To this aim, OASEES' target is to employ a transactional model for the lifecycle of services, which can enable partial provisioning, migration, roll-back and or tear-down of individual components while ensuring service integrity.

***Support for Heterogeneous Dynamic Infrastructure:* Enhanced Platform Awareness** (EPA) [47] is a well-known capability of recent resource management and orchestration systems either in the context of Virtual Machines - VMs (e.g., OpenStack, Open Source Management (OSM)) or in the context of Containers [48]. The challenge here is that cloud computing resources are becoming increasingly heterogeneous and, at the same moment, are distributed widely in across smaller DCs at multiple locations. This trend points to a rapidly increasing adoption of accelerators in the near future. Thus OASEES will enable the discovery and pooling of edge platform acceleration capabilities to create a holistic view of all the different capabilities available in the distributed edge environment and, ultimately, to optimize placement decisions. This can be achieved by leveraging the proposed OASEES agents operating over these heterogeneous infrastructures, platforms and smart devices and collecting device capability information to be stored in OASEES' central repository. OASEES will run customizable optimization algorithms to select the best mapping of the service demands on the physical infrastructure.

Edge Infrastructure Sharing and Monetization: A core OASEES' attribute is also the "sharing" of services across distributed edge-based infrastructures [49], purely suggesting a cross-layer orchestration mechanism between involved network, computation and storage services as already identified by the ETSI MEC Industry Specification Group

(ISG) [50]. In this scope, the Mosaic 5G initiative [51] has already proposed some APIs allowing for an easier cross-domain orchestration of services and federated resource management, while other initiatives work towards achieving a cross-infrastructure collaboration but focusing on more specific layers [52]. The evolution and proliferation of software defined infrastructures allows access and configuration of services through well-defined APIs; to this aim, OASEES intends to combine existing and SotA technologies and techniques so that to develop an E2E cross-domain service sharing framework [53], to achieve optimal resource management/consumption. The developed framework will allow third-party service providers to offer their services through a service marketplace. This capability can be perfectly aligned with the "neutral host" paradigm [54], which has lately become an attractive business model, expanding to 5G/6G infrastructures.

AI-Enabled Data Processing for Hyper-Distributed Applications: Numerous of analytics processes, varying from factory automations to autonomous vehicle operations or safety-critical applications rely on the continuous, low-latency flow and processing of data to generate results within a short timeframe. Especially in production environments with continually evolving data, a deployed ML model is "bound" to degrade in quality without a constant feed of new data feeds, as the assumptions on which it was developed may become less valid with time [55]. Although edge computing seems to be an attractive alternative for such cases, the majority of the existing computing techniques (used in the cloud and/or on premises) are usually not directly applicable to the edge, due to the diversity of computing sources, lack of resource management and distribution of data. However, the provision of the necessary abstraction layers practically "brings" AI tasks "closer" to the source, thus overcoming the most common culprits of cloud computing while, at the same time, benefiting from the enhanced privacy and inherent scalability of distributed edge approaches. Based on this approach, OASEES aims to rely on secure data spaces for storage and privacy-preserving ML technologies (i.e., Federated Learning [56]), allowing users to train and share their models without compromising the sovereignty of their data. Moreover, the edge analytics services shall benefit from increased trust and faster response times to changing environmental conditions (concept/data drifts) through the adoption of MLOps (ML Operations) principles [57] for continuous monitoring, treating ML assets consistently with all other software assets within a Continuous Integration/Continuous Deployment (CI/CD) environment.

Trustworthy and Secure Edge: The highly distributed and heterogeneous nature of the OASEES infrastructure and operating environment dictates architectural design around a form of "Zero-Trust" Architecture [58], as only trustworthy and secure edge nodes shall be authorized to participate. This implicates for deployment of a "mixture" of existing and cutting-edge technologies, such as Trusted Computing attestation [59] and cloud-native secure identities with SPIFFE (Secure Production Identity Framework for Everyone) [60]. The attestation capability of OASEES ensures that only nodes with a trusted hardware, firmware and Operating System (OS) environment shall be used, which prevents from hardware supply chain attacks, bootkits, rootkits and malware. The cloud-native secure identity of a workload is bound to the attestation of the underlying hosting infrastructure, ensuring that only secure and trusted services can participate in the workload.

Blockchain-Backed IoT Governance: The multi-party smart contract deployed on top of blockchain technology [61] sustains the deployment of heterogeneous and dynamic architecture to help orchestrate processes and workflows in the OASEES. Blockchain as a decentralized distributed database enables sharing of trustworthy information among different nodes part of a certified network. Its main technological features are decentralization, availability, information immutability and non-repudiation properties. It considerably improves trust over data processing. OASEES intends to present an agile architecture and supports heterogeneous technological devices that enable easy integration of blockchain technology. The edge and cloud components of OASEES will generate and process different information. Blockchain and smart contracts will serve as a software connector among various architectural components by enabling exchanging a particular set of information in a trustworthy manner. With the help of the smart contract, it will enable decentralized autonomous software agents (Self-Sovereign Identity (SSI) [62]) to play a role in certifying edge and cloud devices, which further can be identified in a decentralized manner by using the notion of a Decentralized Identifier (DID) [63]. That will enable authorizing information exchange as an independent decision-maker, based on specific data sharing policy, performing service automation according to specified requirements. This also covers the management aspect of edge and cloud devices in a decentralized autonomous organization (DAO) way [64], fostering trusted data processing.

4 Use Cases and Pilot Deployments

OASEES has identified the need for a novel, inclusive and disruptive approach regarding the cloud to edge continuum and swarm programmability. To increase expected impact, the project has identified six distinct use cases related to different verticals, as briefly discussed in the following sections. The common features of all proposed approaches is the fact the OASEES proposes: (i) agile and secure architectures for collaborative smart nodes with decentralized or swarm intelligence, which build on European strengths in embedded sensors and devices and wireless communication, both non-cellular and mobile 5G networks; (ii) appropriate programming environments for smart edge-connected nodes and dynamic groups of nodes across the device-edge-cloud continuum, which reduce the complexity of programming and maintenance; (iii) dynamic open environments and tools, which stimulate open architectures and interfaces, interoperability and avoiding vendor-lock-in, and open source where appropriate, and; (iv) solutions to further strength Europe's position in the market of next generation smart systems (sensors and devices) integrated in an evolving IoT and cyber-physical ecosystems with strong capacities at the edge. The proposed use cases are discussed as follows:

Smart Edge-Connected Node for the Analysis of Voice, Articulation and FluencyDisorders in Parkinson Disease: OASEES will develop and test an innovative smart edge-connected sensor, which will be the basis of an interactive and intelligent wearable for the acoustic analysis of voice in Parkinson Disease (PD). Voice alterations and oral communication disorders, especially in articulation, are present in 40–80% of patients with PD. Instrumented voice analysis allows an early identification of these

distortions in order to design or adapt supportive interventions. It also allows the identification of changes in voice parameters for predicting the worsening of disease. OASEES will develop an intelligent edge device capable of sensing, recording and analysing patients' utterances, as well as providing smart, adaptive and personalized guidance on rhythm and intonation. The aim is to develop a system usable both in rehabilitation centres during sessions with therapists and at home. The edge devices will operate and be monitored over the OASEES DAO [65], supporting real-time monitoring of the health information in a trusted and private manner, while allowing the medical practitioner to take the crucial decisions. The devices will operate in the form of swarm and be able to be updated automatically and also leverage the AI edge accelerators for advanced processing and insights.

Electrical Vehicles (EVs) Fleet Coordinated Recharging to Support Optimal Operation of Electricity Grid: In a power infrastructure power network congestions can occasionally take place in the operated electricity grid, which may be dealt with or without any grid reinforcement by leveraging on mobilizing flexibility and stabilization services from local energy consumption stationary (including smart home consumption IoT flexible devices, smart substation devices for decentralized grid monitoring, smart EV recharging stations) and on-the-move-assets (EV fleets).

Electricity produced by renewable sources (photovoltaics - PVs) is usually fed into the low voltage (LV) electricity network and most is consumed by energy customers (i.e. houses, offices, etc.). However, surplus of generated power would generate reverse power flows through the LV distribution network substation which is generally designed to handle only unidirectional electricity flows, thus reverse flows may generate significant issues. To avoid this abnormal operation, electrical vehicles can be offered a dedicated EV fleet platform to "match" their EV charging needs with proper network time and space requirements. This use case will demonstrate the capability of deploying and coordinating in a scalable yet near real-time way the operation and management of swarms of IoT-based devices (e-vehicles), which will be coordinated and programmed through the OASEES SDK and orchestration platform. The involved EV fleet operator and respective EV drivers community manager will optimize EVs' recharging schedule to "address" local technical requirements from the electricity grid operator, in presence of local congestion or local planned or unplanned maintenance of electricity grid branches. The respective pilot will also include smart stationary assets such as smart meters, and smart recharging stations. The EVs will be requested to be charged when surplus of PV generated power is available, with a view to increase the share of self-consumption. The charger will be hence communicating with EV driver and with car battery management system to predict if the requested flexibility will be available in due time.

***Drone Swarm over 5G for High Mast Inspection*:** Autonomous drone inspections can provide tower companies with the data and insights they need to expand their infrastructure. OASEES autonomous drone software will gather high resolution aerial data and generate accurate 3D models and a 360-degree panoramic view of a potential antenna's location. Stakeholders shall be able to: see exactly what is in the line of sight from the location; identify potential obstructions, and; establish the distance from nearby existing antennae. This data can be easily and inexpensively acquired locally – but can be shared

anywhere in the world. The process of acquiring local permits is made dramatically easier when accurate data is shared between tower companies and local regulators. In dense urban areas, tower companies may not be able to develop an entirely new site; in urban environments, tower companies must adapt their existing site to the 5G network needs. Autonomous drone inspections will allow companies to see exactly what that existing equipment is and determine how to utilize the site profitably for the 5G network rollout. A successful operation of drone swarms in a self-organized manner requires the integration of the networking and computational systems, which until now have been mostly investigated in isolation. To this aim, OASEES will integrate the DAO paradigm for the self-organized operation of a drone swarm, which will rely on the tight consolidation of the networking (5G-RedCap [66], 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks)) [67, 68] and edge acceleration technologies (i.e.: SNN). Each of these two systems shall benefit from the presence of the other: for instance, the networking system should be able to find better transmission channels towards neighbors and/or better end-to-end paths towards faraway drones. The SNNs in this case will serve as a power efficient accelerator technology mounted in the drone, to provide fast and accurate detection of mast defects.

Swarm Powered Intelligent Structural Safety Assessment for Buildings: The structural condition of critical infrastructures is usually inferred by processing data from local sensors (mostly accelerometers and laser deformation sensors). There are already in use decision support software (DSS) that collect the structural data and help in decision making in critical times (such as post-earthquake, strong winds, heavy snows, etc.). Currently, the collection of the sensor data takes place in the customer's premises. The data are then transferred to a remote DSS for post-processing and decision making, which is inefficient and causes several practical problems, including data privacy concerns and, most importantly, increased response time. It would be highly beneficial to migrate to a distributed DSS architecture, with components both at the edge and the central cloud. This use case will exploit already installed sensor networks which are feeding data to their DSS. This shall imply for the necessary hardware upgrades and adaptations at the sensor locations, modifications in the local network infrastructure as well as (possible) adaptations to the data acquisition protocols. OASEES will be integrated by: (i) installing the respective edge devices close to the sensors, and; (ii) composing and deploying a distributed DSS application via the use of a dedicated SDK. The sensor data will be locally pre-processed at the edge and then the product will be forwarded to the cloud for high-level monitoring and dissemination. This approach is expected to yield a much more robust system, higher reliability, as well as less dependence on human intervention.

Robotic Swarm Powered Smart Factory for I4.0: In this case, it shall be developed a fully automated system for the production of furniture in all stages of processing, that is: from the standard panel to the assembly of the cabinet where the operator is assisted by industrial anthropomorphic robots for dangerous and low added value tasks, by collaborative robots in the final stages of assembly, insertion of hardware, glue dispensing and finishing, in a safe way, without any need for fences or other barriers, and AMR (Autonomous Mobile Robots) self-driving for flexible interconnections between different cells and islands. In OASEES, the focus of this use case would be the finishing (sanding) machine, designed to satisfy medium and large companies that require the

highest quality: this will deal with sanding of "complex" geometry pieces of furniture (e.g. doors) via an automatic sanding system based on the application of a collaborative anthropomorphic robot. The aim will be about implementing an automated manufacturing process for semi-finished wood panels to be transferred from one station to the sanding machine and from there to the other station via AGVs (Automated Guided Vehicles), coordinated and programmed by the OASEES orchestrator and SDK for line supervision, relieving human operators from burdensome tasks. The essential part in this process is the incorporation of DAO functionality for HITL (Human in the Loop) [69, 70] decision making for I4.0.

Smart Swarm Energy Harvesting and Predictive Maintenance Wind Turbines: Today, the maintenance of wind farms represents a cost of 20% of the total project and this is a determining factor for the viability and durability of the asset. Of major importance are issues about inspection of wind turbine blades and, correspondingly, detection of possible anomalies so that to optimize the operation and maintenance of the turbines. BAMS (Blade Acoustic Monitoring System) is a new system for such sort of inspection and predictive maintenance of wind turbine blades, which is also portable, non-intrusive and independent from the manufacturer. It can "listen" to the wind turbine, acquire the acoustic signals produced when the wind interacts with the blades and detect and identify faults in them, thus improving the performance and operational reliability of the wind turbine. BAMS can detect abnormal operations in the blades such as structural failures, wear, ice, corrosion, or dirt. The key enabler in the seamless integration of smart energy renewable systems to existing infrastructure is smart metering. Blockchain can provide the backend for distributed data structures to securely store transactions in a decentralized manner. In OASEES, novel IoT based meters will be implemented to support on-the-fly programmability. The device swarm will be based upon IoT sound transducer (microphones) applied to wind turbines. The main goal is to extend the capabilities of BAMS, to be able to function as an IoT device in swarm mode. This will allow the simultaneous capture and processing of data from a considerable number of wind turbines thus creating a BAMS network. All the acquired data will be transmitted to the cloud, processed securely, and analyzed using machine learning algorithms so that the sensors are able to learn from each other (improved calibration, noise suppression, etc.), and to improve and obtain better metrics while optimizing the failure prediction on the blades of the wind turbine.

5 Overview

The Open Source community will also be invited to leverage its capabilities for building and managing innovative edge services. The project scope envisions a holistic approach for edge data processing, aiming to disrupt current practices which heavily rely on non-European cloud AI data processing, and "push" AI training and inference at the edge of the network, while being vertical agnostic.

In particular, OASEES targets several specific measurable objectives, each one associated with one – or more – key results, which are in turn accompanied with a set of capabilities and KPIs to be validated during project duration. These are about: (i) designing a decentralized, agile and secure architecture for collaborative smart nodes at the

edge, supporting heterogeneous device communication, backed by the DAO paradigm integration; (ii) building a secure, trustworthy and decentralized edge ecosystem with native device support for a portable digital identity that does not depend on any centralized authority; the related device identity will be a new class of identifier that fulfils requirements for persistence, global resolvability, cryptographic verifiability and decentralization; (iii) structuring rapid development kits (RDKs) for an open programmable framework across different smart edge nodes, while incorporating efficient cloud-to-edge continuum intelligence across heterogeneous target environments; (iv) demonstrating the framework and programmability toolkit in a set of six different vertical use cases and evaluating the benefits across different sectors; (iv) maximizing business impact of the expected results and fostering the creation of an open-source community around the proposed, per case, solutions, engaging a diverse set of stakeholders, to support market viability.

OASEES will be capable to operate in multi-instance (multi-domain) configurations and the corresponding system shall enable the user to: (i) discover and select available platforms, services and capabilities pertinent to their needs; (ii) develop AI services as well as automate lifecycle management operations; (iii) deploy and manage AI workflows across the compute continuum; (iv) configure service performance constraints; (v) interactively explore data and exercise MLOps; (vi) verify the integrity of infrastructure and services across the continuum.

Acknowledgments. This work has been performed in the scope of the *OASEES* European Research Project and has been supported by the Commission of the European Communities */HORIZON, Grant Agreement No.101092702.*

References

1. Gabriel, T., Cornel-Cristian, A., Arhip-Calin, M., Zamfirescu, A.: Cloud storage. A comparison between centralized solutions versus decentralized cloud storage solutions versus decentralized cloud storage solutions using Blockchain technology. In: Proceedings of the 54th International Universities Power Engineering Conference (UPEC'19), pp. 1–5. IEEE (2019)
2. IBM, What is cloud hosting. https://www.ibm.com/cloud/learn/what-is-cloud-hosting
3. Leskinen, J.: Evaluation criteria for future identity management. In: Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'12), pp. 801–806. IEEE (2012)
4. Thakur, M.A., Gaikwad, R.: User identity and access management trends in IT infrastructure - an overview. In: Proceedings of the 2015 International Conference on Pervasive Computing (ICPC'15), pp. 1–4. IEEE (2015)
5. Zareen, M.S., et *al.*: Artificial intelligence/machine learning in IoT for authentication and authorization of edge devices. In: Proceedings of the 2019 International Conference on Applied and Engineering Mathematics (ICAEM'19), pp. 220–224. IEEE (2019)
6. Vorakulpipat, C., et *al.*: Comprehensive-factior authentication in edge devices in smart environments: a case study. In: Proceedings of the 11th International Conference on Control, Automation and Information Sciences (ICCAIS'22), pp. 391–396. IEEE (2022)
7. Lu, Y., Wang, D., et *al.*: Edge-assisted intelligent device authentication in cyber-physical systems. IEEE Internet Things J. **10**(4), 3057–3070 (2023)

8. Castellano, G., Esposito, F., Risso, F.: A service-defined approach for orchestration of heterogeneous applications in cloud/edge platforms. IEEE Trans. Netw. Serv. Manag. **16**(4), 1404–1418 (2019)
9. Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., Sabella, D.: On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration. IEEE Commun. Surv. Tutor. **19**(3), 1657–1681 (2017)
10. Sonmez, C., et *al.*: Fuzzy workload orchestration for edge computing. IEEE Trans. Netw. Serv. Manag. **16**(2), 769–782 (2019)
11. Ranjan, A., Guim, F., Chincholkar, M., Ramchandran, et *al.*: Convergence of edge services & edge infrastructure. In: Proceedings of the 2021 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN'21), pp. 96–99. IEEE (2021)
12. Loghin, D., Ramapantulu, L., Teo, Y.M.: Towards Analyzing the performance of hybrid edge-cloud processing. In: Proceedings of the 2019 IEEE International Conference on Edge Computing (EDGE'19), pp. 87–94. IEEE (2019)
13. Risso, F.: Creating an edge-to-cloud computing continuum: status and perspective. In: Proceedings of the 3rd International Conference on Embedded and Distributed Systems (EDiS'22), p 4. IEEE (2022)
14. Accenture, Edge computing. https://www.accenture.com/bg-en/insights/cloud/edge-computing-index
15. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: Vision and challenges. IEEE Internet Things J. **3**(5), 637–646 (2016)
16. Masip-Bruin, H., Marín-Tordera, E., et *al.*: Managing the cloud continuum: lessons learnt from a real fog-to-cloud deployment. Sensors (MDPI) **21**(9), 2974 (2021)
17. Dietrich, M., Facca, F.M.: Cloud computing in Europe: landscape analysis, adoption challenges and future research and innovation opportunities. Horizon Cloud (2022). https://www.h-cloud.eu/?wpdmdl=4541&ind=1645025986562
18. John, W., Sargor, C., Szabo, R., Awan, A.J, Padala, C., Drake, E., et *al.*: The future of cloud computing. Ericsson Technol. Rev. **2020**, 1–13 (2020)
19. Microsoft Azure Stack Edge. https://azure.microsoft.com/en-us/products/azure-stack/edge/
20. StackPath LLC, What is edge orchestration? https://www.stackpath.com/edge-academy/what-is-edge-orchestration/
21. Hossain, M.D., Sultana, T., Hossain, M.A., Huh, E.-N.: Edge orchestration based computation peer offloading in MEC-enabled networks: a fuzzy logic approach. In: Proceedings of the 15th International Conference on Ubiquitous Information Management and Communication (IMCOM'17), pp. 1–7. IEEE (2017)
22. Wu, Y.: Cloud-edge orchestration for the internet of things: architecture and AI-powered data processing. IEEE Internet Things J. **8**(16), 12792–12805 (2021)
23. Petri, I., Rana, O., Zamani, A.R., Rezgui, Y.: Edge-cloud orchestration: strategies for service placement and enactment. In: Proceedings of the 2019 IEEE International Conference on Cloud Engineering (IC2E'19), pp. 67–75. IEEE (2019)
24. Waguie, F.T., Al-Turjman, F.: Artificial intelligence for edge computing security: a survey. In: Proceedings of the 2022 International Conference on Artificial Intelligence in Everything (AIE'22), pp. 446–450. IEEE (2022)
25. Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., Lv, W.: Edge computing security: state of the art and challenges. Proc. IEEE **107**(8), 1608–1631 (2019)
26. Pujol, V.C., Raith, P., Dustdar, S.: Towards a new paradigm for managing computing continuum applications. In: Proceedings of the 2021 IEEE Third International Conference on Cognitive Machine Intelligence (CogMI'21), pp. 180–188. IEEE (2021)
27. OASEES ("Open Autonomous programmable cloud appS and smart EdgE sensors") Horizon project, Grant Agreement No. 101092702. https://oasees-project.eu/

28. Kim, J.-Y.: FPGA based neural network accelerators. Adv. Comput. **122**, 135–165 (2022)
29. Yamazaki, K., Vo-Ho, V.-K., Bulsara, D., Le, N.: Spiking neural networks and their applications: a review. Brain Sci. **12**(7), 863 (2022)
30. Abdelgaber, N., Nikolopoulos, C.: Overview on quantum computing and its applications in artificial intelligence. In: Proceedings of the 2020 IEEE 3rd International Conference on Artificial Intelligence and Knowledge Engineering (AIKE'20), pp. 198–199. IEEE (2020)
31. Li, Z., Sharma, V., Mohanty, S.P.: Preserving data privacy via federated learning: challenges and solutions. IEEE Consum. Electron. Mag. **9**(6), 8–16 (2020)
32. European Technology Platform for High Performance Computing (ETP4HPC): ETP4HPC Strategic Research Agenda. https://www.etp4hpc.eu/sra.html
33. Balouek-Thomert, D., Gibert Renart, E., et *al.*: Towards a computing continuum: enabling edge-to-cloud integration for data-driven workflows. Int. J. High Perform. Comput. Appl. **33**(6) 1159–1174 (2019)
34. Chen, Q., Gao, C., Fang, X., Luan, H.: Skydiver: a spiking neural network accelerator exploiting spatio-temporal workload balance. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **41**(12), 5732–5736 (2022)
35. Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., Lloyd, S.: Quantum machine learning. Natures **549**(7671), 195–202 (2017)
36. Mahmood, Z.: Fog Computing: Concepts, Frameworks and Technologies. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-94890-4
37. Johnston, D.: The General Theory of Decentralized Applications, Dapps. (2013). https://github.com/DavidJohnstonCEO/DecentralizedApplications
38. Moralis Academy, What is Decentralized AI? The Relationship Between Blockchain and AI. https://academy.moralis.io/blog/what-is-decentralized-ai-the-relationship-between-blockchain-and-ai
39. European Commission, Open Science. https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science_en
40. European Open Science Cloud (EOSC). https://eosc-portal.eu/
41. Vaquero, L.M., Cuadrado, F., Elkhatib, Y., Bernal-Bernabe, J., et *al.*: Research challenges in nextgen service orchestration. Futur. Gener. Comput. Syst. **90**, 20–38 (2019)
42. European Telecommunications Standards Institute (ETSI): ETSI GS NFV-MAN 001 V1.1.1 (2014–12): "Network Functions Virtualisation (NFV); Management and Orchestration". https://www.etsi.org/deliver/etsi_gs/nfvman/001_099/001/01.01.01_60/gs_nfv-man001v010101p.pdf
43. Kreutz, D., Ramos, F.M.V., Veríssimo, P.E., Rothenberg, C.E., et *al.*: Software-defined networking: a comprehensive survey. Proc. IEEE **103**(1), 14–76 (2015)
44. Zhao, Y., Wang, W., Li, Y., Meixner, C.C., et *al.*: Edge computing and networking: a survey on infrastructures and applications. IEEE Access **7**, 101213–101230 (2019)
45. Metsch, T., Edmonds, A., Parák, B.: GFD-R.184 Open Cloud Computing Interface - Infrastructure. Open Grid Forum (OGF), OCCI Working Group, European Commission (2011)
46. OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) Technical Committee (TC). https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca
47. Villarreal Pelegrino, J.: An Introduction to Enhanced Platform Awareness (EPA) capabilities in OpenStack (2020). https://www.juliosblog.com/a-quick-introduction-to-enhanced-platform-awareness-epa-capabilities-in-openstack/
48. Intel, Enhanced Platform Awareness in Kubernetes Application Note (2017). https://networkbuilders.intel.com/solutionslibrary/enhanced-platform-awareness-in-kubernetes-application-note

49. Dustdar, S., Murturi, I.: Towards distributed edge-based systems. In: Proceedings of the 2020 IEEE Second International Conference on Cognitive Machine Intelligence (CogMI'20), pp. 1–9. IEEE (2020)
50. Sabella, D.: MEC: standards and industry associations around edge computing. In: Sabella, D. (ed.) Multi-access Edge Computing: Software Development at the Network Edge, pp. 19–56. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-79618-1_2
51. Wiranata, F.A., Shalannanda, W., Mulyawan, R., Adiono, T.: Automation of virtualized 5G infrastructure using mosaic 5G operator over kubernetes supporting network slicing. In: Proceedings of the 2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA'20), pp. 1–5. IEEE (2020)
52. Valcarenghi, L., Martini, B., Antevski, K., et *al.*: A framework for orchestration and federation of 5G services in a multi-domain scenario. In: Proceedings of the Workshop on Experimentation and Measurements in 5G (EM-5G'18), pp. 19–24 (2018)
53. Addad, R.A., Taleb, T., Bagaa, M., et *al.*: Towards modeling cross-domain network slices for 5G. In: Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM'18), pp. 1–7. IEEE (2018)
54. Froehlich, A.: An introduction to neutral host networks using private 5G. TechTarget (2023). https://www.techtarget.com/searchnetworking/tip/An-introduction-to-neutral-host-networks-using-private-5G
55. Yan, M.M.W.: Accurate detecting concept drift in evolving data streams. ICT Express **6**(4), 332–338 (2020)
56. Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., et *al.*: Towards Federated Learning at Scale: System Design. Cornell University (2019). https://arxiv.org/abs/1902.01046
57. MLOps. https://ml-ops.org/content/mlops-principles
58. Rose, S., Borchert, O., Mitchell, S., Connelly, S.: NIST Special Publication 800-207: "Zero-Trust Architecture". National Institute of Standards and Technology (NIST) (2020). https://nvlpubs.nist.gov › NIST.SP.800-207.pdf
59. Trusted Computing Group: Where Trust Begins – Protecting the Connected Ecosystem (2023). https://trustedcomputinggroup.org/resource/where-trust-begins/
60. Secure Production Identity Framework for Everyone (SPIFFE). https://spiffe.io/
61. McKinsey & Company: What is Blockchain? (2022). https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain
62. Bosch GmbH: Digital identity – enabling secure collaboration with blockchain technology (2023). https://www.bosch.com/stories/self-sovereign-identities/
63. World Wide Web Consortium (W3C): W3C Recommendation: "Decentralized Identifiers (DIDs) v1.0" (2022). https://www.w3.org/TR/did-core/
64. Buterin, V.: DAOs, DACs, DAs and More: An Incomplete Terminology Guide [Blog post]. Ethereum Foundation Blog (2014). https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/
65. Hassan, S.: Decentralized autonomous organization. Internet Policy Review **10**(2), 1–10 (2021)
66. EverythingRf: What is 5G RedCap? (2020). https://www.everythingrf.com/community/what-is-5g-reduced-capability-or-5g-redcap
67. Bertenyi, B.: 5G evolution: what's next? IEEE Wirel. Commun. **28**(1), 4–8 (2021)
68. McGee, K., Collier, M.: 6LoWPAN forwarding techniques for IoT. In: Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT'19), pp. 888–893. IEEE (2019)
69. Google: Human-in-the-Loop Overview. https://cloud.google.com/document-ai/docs/hitl
70. Bisen, V.S.: What is Human in the Loop Machine Learning: Why and How Used in AI? (2020). https://medium.com/vsinghbisen/what-is-human-in-the-loop-machine-learning-why-how-used-in-ai-60c7b44eb2c0