Review

A Survey on the Computing Continuum and Meta-OS Systems: Perspectives, Architectures, Outcomes, and Open Challenges

Panagiotis K. Gkonis *, Anastasios Giannopoulos, Nikolaos Nomikos, Lambros Sarakis, Vasileios Nikolakakis, Gerasimos Patsourakis, Panagiotis Trakadas

Posted Date: 2 December 2025

doi: 10.20944/preprints202512.0281.v1

Keywords: meta-Operating Systems; cloud continuum; machine learning; Internet of Things; security and privacy

 doi:10.20944/preprints202512.0281.v1

Review

A Survey on the Computing Continuum and Meta-OS Systems: Perspectives, Architectures, Outcomes, and Open Challenges

Panagiotis K. Gkonis [1,*], Anastasios Giannopoulos [2], Nikolaos Nomikos [3], Lambros Sarakis [1], Vasileios Nikolakakis [2], Gerasimos Patsourakis [2] and Panagiotis Trakadas [2]

[1] Department of Digital Industry Technologies, National and Kapodistrian University of Athens, Evripus Campus, 34400 Euboea, Greece

[2] Department of Ports Management and Shipping, National and Kapodistrian University of Athens, Evripus Campus, 34400 Euboea, Greece

[3] Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Samos, Greece

* Correspondence: pgkonis@uoa.gr

Abstract

The goal of the study presented in this work is to analyze all recent advances in the context of the computing continuum and meta–operating systems (meta-OSs). The term continuum includes a variety of diverse hardware and computing elements as well as network protocols, ranging from lightweight internet of things (IoT) components to more complex edge or cloud servers. To this end, the rapid penetration of IoT technology in modern era networks along with associated applications poses new challenges towards efficient application deployment over heterogeneous network infrastructures. These challenges involve among others the interconnection of a vast number of IoT devices and protocols, proper resource management, as well as threat protection and privacy preservation. Hence, unified access mechanisms, data management policies and security protocols are required across the continuum to support the vision of seamless connectivity and diverse device integration. This task becomes even more important as discussions on sixth generation (6G) networks are already taking place, which they are envisaged to coexist with IoT applications. Therefore, in this work the most significant technological approaches to satisfy the aforementioned challenges and requirements are presented and analyzed. To this end, a proposed architectural approach is also presented and discussed which takes into consideration all key players and components in the continuum. In the same context, indicative use cases and scenarios that are leveraged from a meta-OS in the computing continuum are discussed as well. Finally, open issues and related challenges are also discussed.

Keywords: meta-Operating Systems; cloud continuum; machine learning; Internet of Things; security and privacy

1. Introduction

The rapid growth of the number of interconnected devices on the internet (Internet of Things – IoT) has posed new challenges on the design and implementation of flexible network architectures that can handle both a vast number of IoT components (i.e., proper access and resource management protocols) as well as associated security threats [1,2]. In the early years of IoT technology, data generated in the IoT devices was forwarded directly to the cloud domain via classical network infrastructure. However, this strategy can impose certain limitations, mainly related to the increased round trip time in cases of delay sensitive and latency critical applications. Moreover, technological

 doi:10.20944/preprints202512.0281.v1

advances in the IoT domain have made feasible the deployment of advanced services and applications that do not simply rely on data gathering and processing from the IoT network but actively participate in process optimization. Typical examples include automation sensors in industrial 4.0 scenarios as well as smart building sensors. Hence, the need for reduced latency is inextricably combined with the ability to perform time consuming calculations at the edge of the network [3,4].

Over the last decade, a new architectural approach has emerged, leveraging the so-called IoT-Edge-Cloud (IEC) paradigm [5,6]. In this context, edge servers located near the IoT devices process related data and perform time consuming calculations, depending on their computational capacity. The outcomes of these calculations (i.e., encryption procedures, optimization of key performance indicators, training of a machine learning – ML model or creation of blockchains) are send directly to the IoT devices, without the need for central cloud processing and long round-trip times. To this end, the cloud domain either receives corresponding results at a later stage, or it is directly involved in cases of high complexity calculations. Hence, mean response times can be significantly reduced with respect to centralized cloud domain processing. All devices that constitute this complex IoT, edge and cloud ecosystem, are also referred to as the computing continuum. In comparison to single vendor clouds or hybrid clouds centrally managed, heterogeneous IoT devices, data, network, edge and cloud components are significantly more complex to manage, since the continuum integrates a variety of diverse hardware and software elements. To this end, the addition of new devices and protocols can be a scalability-challenging task. The continuum needs to be efficiently managed to optimally meet the application demands during service execution, by not only bringing computation closer to where the data is produced, but also by placing and formatting the data to optimize the execution, both for real-time services and non-real time data analytics [7,8].

In this context, a high-level view of the IEC concept is depicted in Figure 1. The lower layer includes IoT devices as well as user equipment. All these items generate a vast amount of heterogeneous data that needs to be stored and processed accordingly in a secure and privacy preserving way. Moving a step forward, the next layer includes the on-premise layer. To this end, processing nodes with improved computational capacity are located within the premise, e.g. a stadium, an enterprise or a smart home. This can be highly beneficial in industrial scenarios for example, where on one hand sensitive data remains within the facilities of the enterprise and on the other hand latency times can be significantly improved. In the far and near edge layer, high computing nodes that are in close or far proximity to the cloud servers gather data and train advanced ML algorithms and in general perform time consuming calculations. In this context, certain tasks that require high computational power can be offloaded from the on-premise servers. In the cloud domain, a two-fold process is carried out: a) ML model aggregation and update from the individual models that were constructed in the previous layers and b) large scale data processing that was not made feasible in the previous steps due to limited resources.

As the concept of IEC systems is gradually developing, various research efforts have dealt with operating systems and policy configurations than span across this continuum. To this end, diverse challenges are dealt with, such as access to continuum, flexible usage of resources and optimum resource management, performance improvement, threat prediction and mitigation, etc. [9,10]. In the same context, intelligent edge computing and ML are also two promising approaches that can leverage the deployment of the continuum in lightweight devices [11,12]. All the aforementioned topics may represent highly demanding tasks, not only due to the continuum being intrinsically heterogeneous, volatile, distributed and increasingly cognitive, but also due to emerging requests to be open und collaborative. A holistic approach towards the solutioning of this technological trend in future systems can be achieved by architecting, designing and implementing the continuum as extensible, open, secure, adaptable, artificial intelligence (AI)-powered as well as highly performant and technology agnostic.

The goal of the study presented in this work is to analyze all recent developments in the context of meta-OSs and the computing continuum. In this context, various recent works are presented and

 doi:10.20944/preprints202512.0281.v1

analyzed, with respect to the aforementioned challenges and proposed technological solutions. Moving a step forward, a high-level architectural view of a meta-OS system is presented as well, along with indicative use cases and scenarios.

The rest of this work is organized as follows: In the remaining part of the introductory section, related surveys are discussed with respect to their key outcomes. Afterwards, the contribution of our work is highlighted as well. In Section 2, key enabling technologies as well as associated challenges in the computing continuum and meta-OSs systems are described. These include ML, security by design, coexistence with sixth generation (6G) networks as well as data management strategies. Moving forward, in Section 3 all recent developments are presented with emphasis on data access and management protocols, security mechanisms and proposed architectures. In Section 4 a discussion takes place on the key findings of the presented works. Based on this discussion, open issues and future directions are identified. In the same context, a high-level approach of a proposed architectural concept is presented, as previously mentioned. Indicative use cases are described in Section 5. These include process optimization in industrial 4.0 environments, efficient load forecasting in smart grid applications, smart cities as well as optimization of key parameters in railways and in general in critical infrastructures. Finally, concluding remarks are highlighted in Section 6. A schematic overview of the structure of our work for illustration purposes is depicted in Figure 2.

1.1. Related Surveys

In this subsection, indicative recent related survey papers are presented with respect to their key outcomes. To this end, in [13] a survey is provided for cloud-edge workload orchestration at the edge. The orchestration of workloads can be a quite challenging task, due to the heterogeneity of computing equipment in edge scenarios. As the authors correctly point out, a potential solution lies in the creation of lightweight versions of Kubernetes. Another promising approach is the use of *KubeEdge* [14], that is specifically designed for edge applications, instead of trying to reduce the size of Kubernetes. However, as the authors indicate, containers can have certain disadvantages that are mainly associated with large image size and non-robust security. Hence, an alternate approach includes the virtualization of workloads.

In [5], a survey on IEC systems is provided, which focuses on key enabling technologies as well as on the presentation of all recent works on the field. In the same context, limitations and open challenges are discussed as well. To this end, indicative use cases are also presented that are leveraged from the IEC concept. In [15], all latest architectural approaches in computing continuum systems are described. In particular, this work focuses on AI for applications deployed at the edge as well as for efficient AI techniques to manage the workload in the edge of the computing continuum.

 doi:10.20944/preprints202512.0281.v1

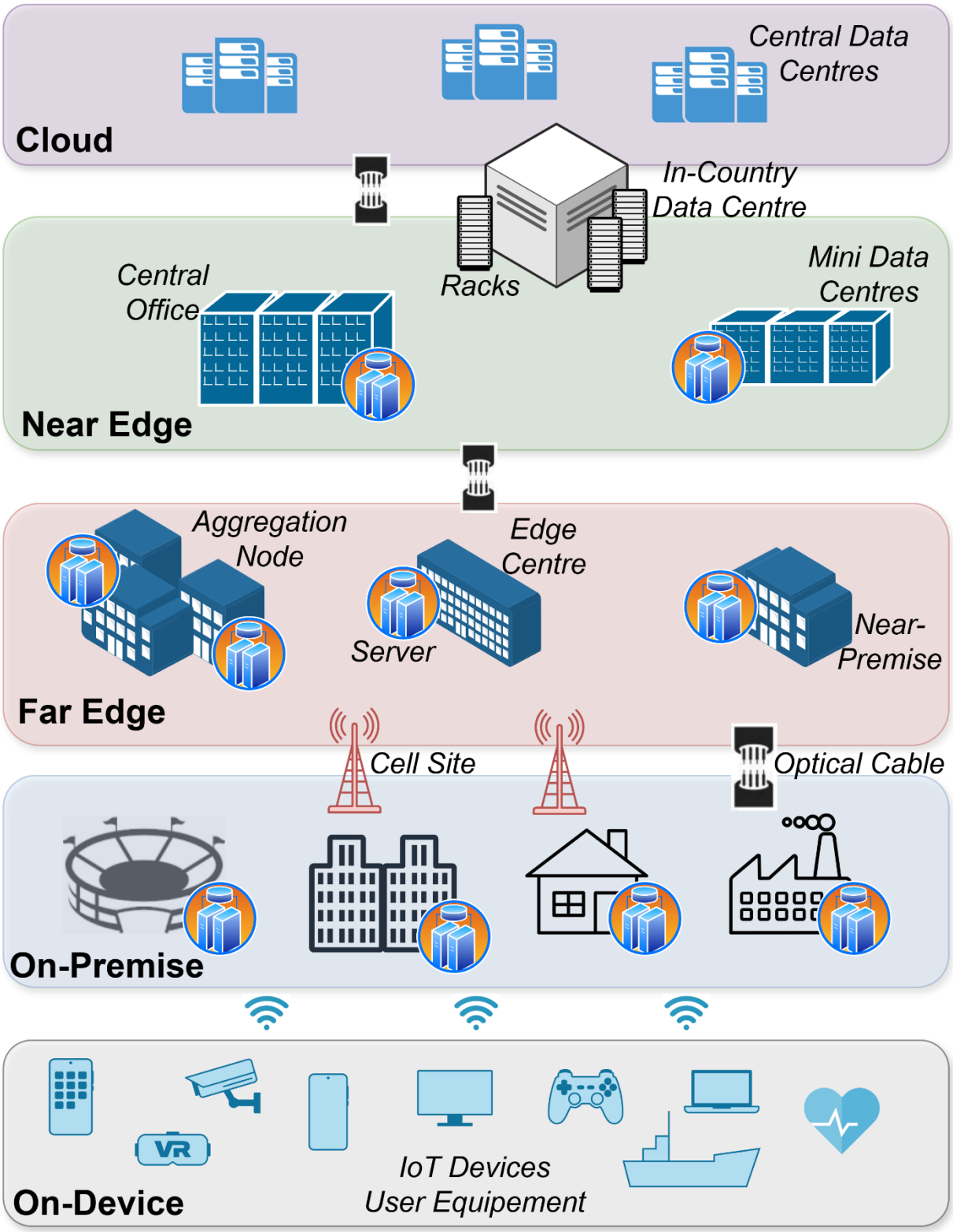

Figure 1. The IoT–Edge-Cloud concept disaggregated in five computing tiers.

In [16], the general architecture of distributed computing systems (DCS) is presented. In the same context, the authors describe various potential applications as well that are based on DCSs. These include among others industry automation, transportation systems, mobile robots, smart cities and health care. In [17], this survey paper analyses all recent trends of computing continuum systems. In this regard, potential use cases include highly mobile self-driving vehicles, holographic streaming services (Telepresence), ultra-reliable industrial IoT as well as urgent computing. In the same context,

 doi:10.20944/preprints202512.0281.v1

various open issues are also discussed, that include among others proper resource allocation and management, simulation tools for large scale performance evaluation, the integration of mobility in the continuum as well as programming distributed applications.

Finally, the survey in [18] focuses on the applications of software defined networking (SDN) as well as network function virtualization (NFV) in the management, orchestration and load balancing of workloads in cloud/edge orientations. Various challenges are also identified, such as distributed architectures, dynamic offloading of resources, security and privacy, intelligent orchestration and work management. The key outcomes of each survey presented are also depicted in Table 1, where open issues and limitations are highlighted as well. To this end, the main points of our work are indicated as well.

Table 1. Indicative related surveys.

Paper	Year	Key Directions	Limitations and Open Issues
[5]	2023	IoT-Edge-Cloud Systems	Focus is on IEC systems and not on access or data management architectures in the continuum
[13]	2023	Cloud Edge orchestration at the edge	Evaluation of containerization or virtualization in real world scenarios
[15]	2024	AI on the edge	Cloud – Edge orchestration Hardware integration to support advanced AI/ML applications
[16]	2023	Architecture of distributed computing systems	Learning Models Intelligent protocols for effective resource management
[17]	2025	Recent trends in computing continuum systems	Flexible resource allocation Mobility in the continuum
[18]	2025	SDN and NFV in cloud edge orientations	Performance evaluation in real world orientations
Our work	-	Architectural approaches of meta-OSs for the computing continuum	-

1.2. Contributions of This Work

In the works that were presented in the previous subsection, emphasis was provided on different parts of the cloud computing continuum (i.e., AI/ML deployments, containerization, virtualization, IEC and DCC architectures, NFV and SDN solutions, etc.). Therefore, unlike other similar works in literature, our work tries to cover all individual aspects in the context of meta-OSs in the computing continuum. These include among others the presentation of the most important key enabling technologies, as well as all related research efforts in data management, security and privacy, as well as resource optimization via ML. To this end, emphasis is given on the analysis of various European Union-funded projects. Therefore, the main contributions of our work can be summarized as follows:

- Investigation into all recent trends in architectural approaches on the integration of meta-OSs with the computing continuum.
- Emphasis on key enabling technologies such as security by design, coexistence with 6G networks, data management, as well as advanced AI/ML approaches that leverage response times and provide optimum resource management.
- A reference architectural approach is presented that takes into account all major players in the computing continuum and their interactions.
- Indicative use cases are presented as well that benefit from the cloud computing continuum.
- Finally, open issues are also identified to trigger further research activities.

 doi:10.20944/preprints202512.0281.v1

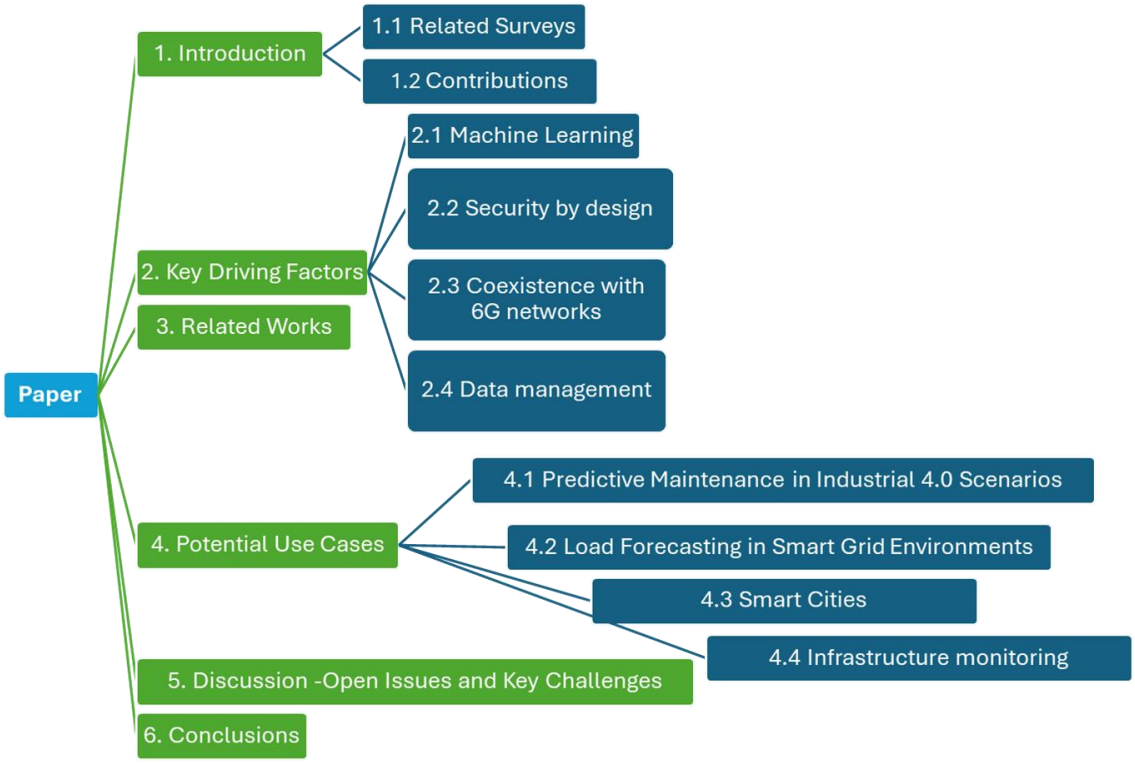

Figure 2. Structure of the present work.

2. Key Driving Factors

Meta-OSs and the computing continuum face numerous challenges that need to be dealt with, as described in the introductory section. The interconnection of numerous diverse devices on one hand necessitates common access and data management protocols and on the other hand brings to front more robust security and privacy protection mechanisms, since the attack landscape is now significantly increased compared to previous generations of wireless networks. To this end, various key enabling factors can be identified, such as efficient AI/ML approaches for proper resource optimization as well as security and privacy protection, security by design, coexistence with 6G networks as well as data management.

2.1. Machine Learning

A challenging research field in the design of the computing continuum systems is the use of appropriate ML approaches both for threat prediction and mitigation as well as for resource optimization. In the latter case, the goal is to select the appropriate architectural layer (i.e., IoT, edge, cloud) and corresponding device where a certain task will be executed. This decision is based on numerous factors, such as task complexity, delay tolerance, energy consumption, etc. Hence, to this end, an efficient ML approach that can adapt to dynamic network orientations is deep reinforcement learning (DRL) [19,20]. In this context, a mobile agent interacts with the environment and selects the appropriate action for the task under consideration, according to a policy that maximizes overall reward. Depending on the outcomes of this action, either positive or negative rewards are given to the mobile agent. After a sufficient number of training rounds, near optimum decision goals can be achieved with the help of neural networks (NNs) that can be trained according to various pairs of potential states and actions. In this context, a quite popular approach is Q-learning, where the agent keeps a score of quality values that are updated after each system transition. To this end, the new q-value is based on the previous q-value and the received reward properly weighted.

A schematic overview of this approach is depicted in Figure 3. To this end, various data are gathered from the IoT devices, the edge controllers and the cloud and are sent to the DRL agent.

 doi:10.20944/preprints202512.0281.v1

These data are related to distinct operational factors, such as historical load, task features as well as current load in the participating devices. The aforementioned approach can be easily applied in Federated Learning (FL) scenarios as well [21]. As depicted in Figure 4, multiple participating nodes that represent either IoT, edge or cloud domains train locally an ML model, based on the data collected from their surrounding environment. Afterwards, ML model parameters, such as weights in case of NN training, are send to the master ML server for model aggregation and update. At this stage, model inference can take place as well. The master server, after processing and aggregating all parameters, sends the updated weights to the participating nodes. Therefore, on one hand computational burden is divided among the participating nodes, and on the other hand no sensitive data is transmitted. Hence, privacy sensitive applications, such as e-health can now be deployed more easily.

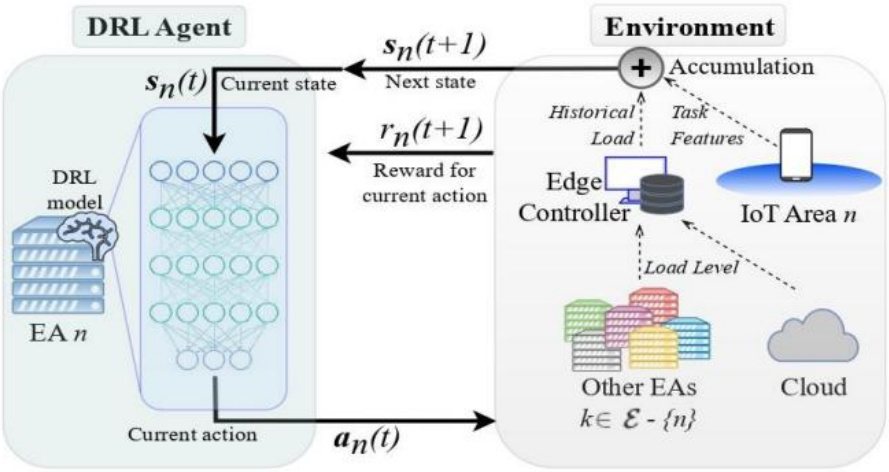

Figure 3. Deep reinforcement learning approach in IoT–Edge–Cloud systems for a given agent $n \in \mathcal{E}$. EA: Edge Agent; $\mathcal{E}$ is the set of DRL edge agents.

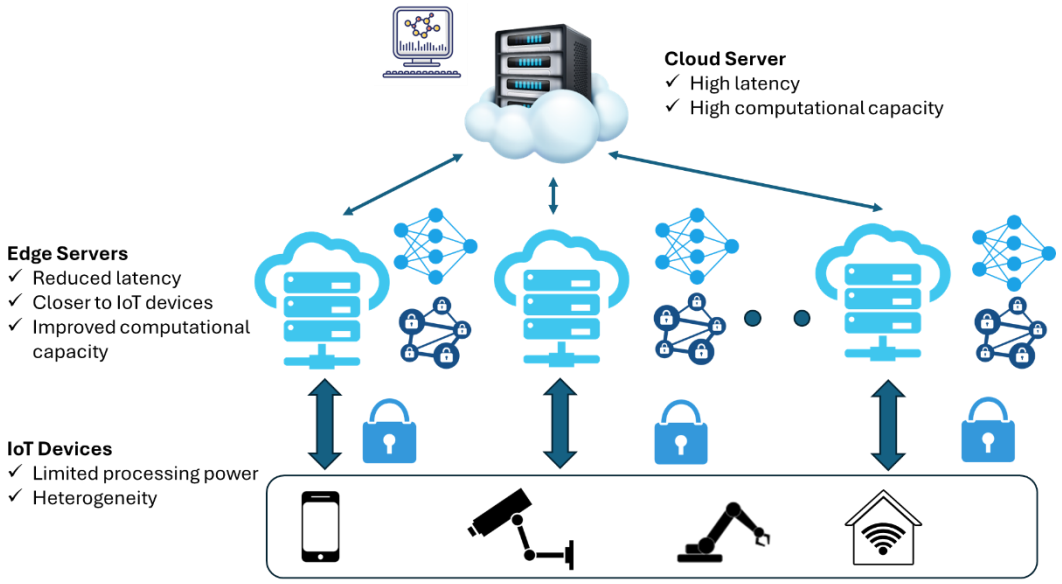

Figure 4. Federated Learning in the computing continuum with local training steps performed at edge layers and model aggregation implemented at the cloud.

2.2. Security by Design

 doi:10.20944/preprints202512.0281.v1

Another challenging research field in the management of the computing continuum is the provision of security by design during application execution. Since this continuum integrates various resource constrained IoT devices, not all of them have the capability to execute advanced security protocols. Hence, various associated security challenges can be identified, such as protecting against unauthorized access, ensuring data security and isolation in a multitenant environment as well as securing virtual machines (VMs) [22,23].

The use of virtualized network elements, open interfaces and disaggregation that are extremely important in the cloud computing era, can pose several security challenges. Unlike for example fifth generation (5G) networks, where security solutions across all devices and base stations are configured with universal settings for certain types of attacks, it is apparent that such an approach cannot be applied in an integrated IEC infrastructure. In this case, the high diversity in service and application provision, connected devices and associated protocols in heterogeneous networks as well as the various physical layer encoding and transmission techniques, render a highly complex environment with different requirements and settings. Since each scenario may have unique security requirements and energy availability, the selection and configuration of security strategies need to be optimized in an adaptive and dynamic manner. As it will be also discussed in the following subsection, cloud computing continuum is envisaged to coexist with 6G networks to support advanced services and applications. The security attacks in 6G networks are polymorphic in nature and sophisticated, using previously unseen custom code, able to communicate with external command and control entities to update their functionality or even implement themselves entirely from code fragments that they intelligently harvest from benign programs, scripts and software blocks already present in the security system in place [24,25]. Therefore, on one hand it is important to have strong security mechanisms in the computing continuum domain, such as the zero trust concept [26], and on the other hand to effectively design ML approaches that can create the appropriate intents in due time for a variety of potential attacks.

2.3. Coexistence with 6G Networks

It is expected that the 6G concept will be based on a holistic integration of broadband networks and lightweight IoT devices that can leverage various cutting-edge applications in the real world. Hence, the underlying infrastructure of the computing continuum as well as meta-OSs should be able to adapt to 6G network protocols, and in particular the ones that are related to proper resource management and security. Typical advanced applications include among others autonomous driving, where high precision sensors are mounted on vehicles, e-health applications with wearable sensors and IoT devices as well as industrial robotic applications [27,28]. In the same context, another promising novelty of 6G networks will be the subnetwork concept, where a network component in the edge acts as a serving access point (AP) in case where connection with the main core network is lost [29,30]. Therefore, in this case, efficient task offloading and reduced latency computations in the edge/cloud domain are of utmost importance, to support critical applications. Moreover, as also referred in the previous subsection, in the case of 6G networks an increased attack landscape should now be dealt with. Hence, efficient network monitoring is required for threat prediction and mitigation via the creation of appropriate intents.

Finally, in the framework of 6G networks, a promising architectural approach that has emerged over the last years is the organic concept [31]. To this end, the long-term vision is to support the ability of 6G networks to dynamically adapt their resources according to user needs and traffic demands, within the available infrastructure resources. Hence, more flexible resource management can be supported, by leveraging the well-known concept of service-based architecture (SBA) of 5G networks. Hence, the meta-OS in the computing continuum should provide the appropriate mechanisms for dynamic device onboarding and detachment from different segments of the network, flexible data gathering, as well as ML model adjustment.

2.4. Data Management

 doi:10.20944/preprints202512.0281.v1

An efficient data management solution should address the requirements of heterogeneous and changing infrastructures by supporting dynamic and flexible data federation between devices, enabling the integration of data from independent and volatile sources within a single application. It will also enable the execution of parts of a service within the data platform to increase performance and favour privacy and will facilitate the development of services to be deployed on the continuum by abstracting data distribution, communication and management details across the different layers of the infrastructure.

In [32] for example, a Message Queuing Telemetry Transport (MQTT) broker has been used for the communication of devices in the IEC continuum. The key features of MQTT are minimal network bandwidth usage, efficient message delivery, and support for a range of quality of service (QoS) levels to ensure message reliability. As the authors point out, although MQTT helps in reducing system vulnerabilities and facilitating compliance with data privacy requirements, there are still various open issues to be addressed with. These include integration with emerging technologies, such as FL, DevOps, and more adaptive security policies for dynamic IoT environments.

Another important issue that should also be considered in the design of an efficient data management system is legislative measures governing data sharing and privacy [33]. Hence, data protection laws should be considered in the new ecosystem via the integration of modules that enable compliance with data protection regulations while transferring the data across the continuum.

A schematic overview of the most important key driving factors in the design of computing continuum systems is also depicted in Figure 5, for illustration purposes.

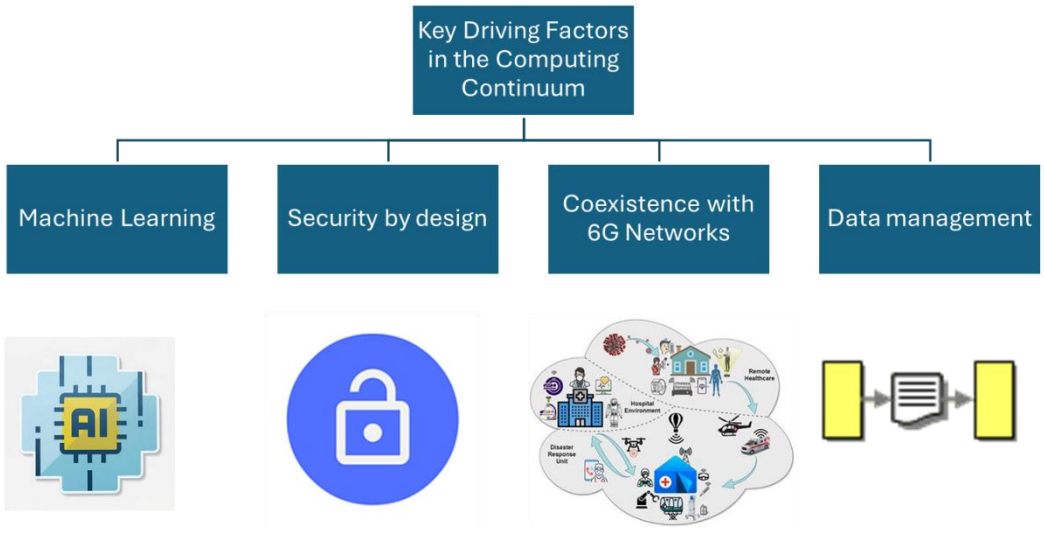

Figure 5. Key driving factors in the computing continuum.

3. Related Works

In this section, various recent works in the context of meta-OSs and the computing continuum are discussed. In [34], and in the context of the EU-funded project FLUIDOS [35], an AI driven approach is presented, to optimize resource allocation during application execution. To this end, a user may ask for the execution of a specific workflow, that is passed by the Operator API to the corresponding ML component. This component is trained using previous experience from similar user requirements. Consequently, this workload is translated to an equivalent set of resources to be committed during service execution. Performance evaluation took place with the help of two well-known datasets and results were compared against the baseline approach (brute-force). In all cases, resource allocation times were significantly reduced.

 doi:10.20944/preprints202512.0281.v1

In [36], the NebulOuS architectural vision is presented and described, for secure and optimal application provisioning [37]. In this context, a model driven approach is presented, where a user first describes an application and the required resources using a well-defined application model. In the same context, admin users also advertise their resources using NebulOuS. Hence, the continuum also acts as a gateway where different entities make use of heterogeneous resources. AI-driven threat detection and mitigation is also supported. In [38], the work presented by the authors is based on the EU-funded project NEMO [39]. To this end, the NEMO approach is based on the Artificial Intelligence of Things (AIoT) - an integration of AI with the physical world. AIoT devices can potentially act as semi-autonomous devices, thus reducing overall network burden as well as latency times. NEMO introduces an open-source meta-OS, that tries to leverage a variety of novel cutting-edge technologies, such as transfer learning (TL) and FL. The concept of AIoT can be highly beneficial in various time sensitive applications, such as in the immediate termination of wind turbines in cases of high-speed winds, shutting down machines in latency demanding industrial 4.0 scenarios as well as helping autonomous vehicles to avoid fatal collisions.

In [40], the concept of IoT Computing Continuum, or IoTinuum is introduced. To this end, multiple computing servers are distributed across the IoT continuum to leverage latency critical calculations. Hence, depending on the application, some sensors may forward data directly to the cloud or others to use the processing nodes. In this context, the IoTinuum is composed of 6-stages: The S1-thing, which includes all physical layer components, such as sensors and actuators, the S2-Mist stage that includes all low power computing nodes in close proximity to the S1-devices, the S3-Fog stage that includes high computing nodes that can be located far away from sensor nodes and the S4-Cloudlet that is composed of a reduced set of servers running as a micro datacentre closer to the cloud. Finally, the architectural approach also consists of the S5-Cloud and S6-App, where the later one includes all smart applications. In this context, two use cases are analysed, and in particular smart drone delivery as well as smart structural monitoring. In [41], the concept of 6G Computing Continuum (6GCC) is introduced, where a realistic testbed has been used. To this end, a large-scale cell free AP network is evaluated, for large scale highly demanding computations.

In [42], a domain-agnostic approach is presented, capable of supporting heterogeneous devices in various network environments. The key advantages of this approach are among others a peer-to-peer continuum instead of a hierarchical one, dynamic orchestration of resources, distributed and decentralized learning instead of centralized approaches, as well as context-aware solutions. To this end, various application scenarios are presented as well, such as smart charging stations for electric vehicles, energy reduction towards carbon-neutral manufacturing processes, just-in-time arrival for vessels, as well as green driving for reduced fuel consumption and decreased vehicle emission.

In [43], a novel DRL approach is discussed, for task offloading in cloud-edge continuum (CEC) systems. Based on this framework, autonomous decisions can be made based on local conditions while dynamically adapting to changing network environments. In this context, task latency and drop rates are optimized, where DRL agents are employed at each edge server. Performance evaluation indicates that significant improvements were achieved compared to baseline methods. As the authors correctly point out, future directions include the extension of this framework to dynamic environments, as well as the creation of a parallel framework to enable fast decision procedures in the IoT devices. The work in [44] presents an optimization framework for smart homes energy consumption based on FL. A key novelty of the presented approach is that FL aggregation is not based on simple averaging of the produced models. Instead, newly created data contribute more on the produced global model. The results demonstrate that the proposed method performs similarly or better than other models in terms of prediction error. The last two cited works have been carried out in the context of the EU-funded ICOS project [45].

In [46], a novel concept of self-distributing systems (SDSs) is presented and evaluated. To this end, code mitigation of an application can take place in various resources of the computing continuum. Performance is evaluated against other baseline approaches as well as with respect to serverless computing. In this context, an agent which is located on top of the proposed four-layered

 doi:10.20944/preprints202512.0281.v1

architectural approach performs DRL to extract the optimum subset of resources for code mitigation. As the authors indicate, scalability of this approach as well as evaluation in more complex scenarios is a challenging research field for further research.

In [47], a novel symbiotic computing model is introduced, where all participating members in the cloud continuum may share common resources for task improvement. To this end, two approaches are considered, non-cooperative and cooperative resource pricing. In [48], a discussion takes place on containerization and virtualization approaches, in the cloud computing continuum. On one hand, containers can be deployed more easily in lightweight IoT devices, however they are more vulnerable in security attacks. On the other hand, VMs can offer complete isolation during application execution at the cost of increased hardware requirements. In [49], the problem of optimum planning in multi-area, multi-service and multi-tier edge cloud computing environments is investigated. To this end, an optimization problem is formulated and solved based on matrix adaptation.

In [50], two novel reference architectures are presented: one for edge–cloud computing models and the other for edge–cloud communication technologies. In the same context, indicative use cases are presented as well. In [51], and in the context of the project NEMO, the open-source framework is described. To this end, various key functionalities such as security, AI, service and data management, meta-orchestration and resource management are provided as open-source components. In [52], security in the continuum is leveraged with the help of physical unclonable functions (PUFs). These kinds of functions are generated using the unique digital identifiers derived from the inherent variability in the manufacturing process of integrated circuits, as a way to enhance security mechanisms at minimal overhead cost [53]. Therefore, in this work a lightweight PUF generation method is introduced, that can be applied even in cases where only one of the two involved parties can support PUFs. In the same context, a security as a service (SaS) framework is introduced, based on the Chef software [54].

In [55] the *Ratio1* meta-OS is presented. The key features include decentralized ML as well as device authentication. As the authors point out, large-scale meta-OS deployments along with more advanced privacy policies can trigger further research activities. In [56] an interconnection framework is presented that can leverage seamless operation of large IoT deployments. This framework uses the Sirius tool and Acceleo, where a smartphone-centric gateway application is used as a mediator to connect devices and sensors within an IoT environment. Finally, in [57], the COGNIFOG concept is presented [58], which is an open-source framework that tries to leverage decentralized ML and decision making and distributed computing. To this end, container-based virtualization is favoured, which is a lightweight and secure alternative that also supports the microservice concept.

All the aforementioned works along with their key directions, limitations and open issues are presented in Table 2 as well.

Table 2. Related works.

Paper	Year	Key Directions	Limitations and Open Issues
[34]	2024	Presentation of the FLUIDOS Project AI optimization during application execution	Deployment in real-world scenarios
[36]	2023	Presentation of the NebulOus project	Performance evaluation in real world scenarios
[38]	2024	Presentation of the NEMO Project Open-source components for various features (e.g. AI, security, service and data management)	Performance evaluation in large scale scenarios
[40]	2024	Six proposed stages of the IoT Computing Continuum	Integration of programmable network stages
[41]	2022	6G Computing Continuum	Integration of the computing

 doi:10.20944/preprints202512.0281.v1

			continuum with 6G architectural approaches
[42]	2022	Presentation of the RAMOS concept	Context aware machine learning
[43]	2024	Task offloading in IoT Cloud Edge scenarios via DRL	Extension in dynamic topologies Additional performance metrics during optimization
[44]	2023	Federated learning in IoT scenarios	Evaluation in additional real-world scenarios
[46]	2023	Application resources distribution in the computing continuum	Evaluation of the SDS approach in more complex scenarios Scalability
[47]	2025	Resource pricing in computing continuum	More diverse user behavior scenarios
[48]	2024	Virtualization vs. Containerization in the cloud continuum	Performance evaluation of bigger hardware architectures for Edge or Cloud Security issues in both approaches
[49]	2025	Edge-Cloud Continuum Planning	Integration of AI techniques
[50]	2024	Edge cloud computing and communication	Efficient communication technologies for the different parts of the continuum
[51]	2024	Open-source framework of NEMO project	Performance evaluation in large scale scenarios
[52]	2023	Physical Unclonable Functions	Evaluation in realistic scenarios
[55]	2025	*Ratio1* meta-OS Decentralized ML and device authentication	Additional privacy policies Broader cross-chain interoperability
[56]	2023	Large scale interconnection of IoT devices	Only one smartphone was used for performance evaluation Additional testing with diverse IoT devices
[57]	2025	The COGNIFOG framework	Orchestration intelligence Decentralized, privacy-preserving AI training at the edge

4. Discussion - Open Issues and Key Challenges

From the discussion of the previous section various open issues and key challenges can be identified in the context of the computing continuum. A key outcome of the presented works is that performance evaluation in realistic scenarios is still a challenging issue. All approaches so far are based on publicly available datasets or on limited network topologies and testbeds. Another key aspect that was also highlighted is to effectively interconnect a vast number of heterogeneous devices and protocols via secure open access interfaces. The seamless support of highly demanding applications necessitates proper resource management, which is made feasible only via efficient ML approaches. However, the IEC continuum is a highly dynamic environment, where new elements are constantly added/removed from the network; hence constant updates of the ML models are required. To this end, and in order to avoid frequent retraining of the derived models, TL can be highly beneficial [59]: The obtained knowledge from another task and dataset (even one not strongly related to the source task or dataset) is transferred to the task under consideration to reduce learning costs. In the same context, the increased number of devices and associated protocols poses new challenges in the design and implementation of efficient security algorithms, since threat landscape is significantly increased. Hence, ML model training is now a multi-dimensional task, since apart from resource optimization the creation of intents for network recovery after attacks is also of utmost

 doi:10.20944/preprints202512.0281.v1

importance. However, a trained ML model that provides near optimum results for the first task (i.e., resource optimization) might not be the ideal one for threat mitigation and vice versa.

Therefore, based on the previous discussion, various key challenges can be identified as well, which are summarized below:

- ML model deployment on lightweight IoT devices. In the IEC continuum, the goal is to offline train an appropriate ML model either at the edge or in the cloud and then deploy it on the IoT device. However, not all IoT devices have the processing capability to run hardware consuming ML models. Hence, appropriate tiny ML models can be deployed that can effectively run in small IoT devices [60]. In the same context, as previously mentioned, different models may provide near optimum results for different tasks. In this case, ML repositories in edge and or cloud servers are created and ML model deployment in lightweight IoT devices might occur for more than one trained model, which unavoidably poses additional computational requirements.
- As also mentioned in the key challenges section, the integration of computing continuum implementations with 6G architecture is a challenging research field, as it will allow the seamless integration and coexistence of various cutting-edge technologies. However, as the landscape of connected devices increases, security concerns may become a major issue, as previously mentioned. Flexible network architectures allow the identification of multiple types of attacks [61]. To this end, either predictive or mitigation actions can be supported both for well-known as well as for zero-day attacks, with the help of additional emerging technologies, such as digital twins. In the same context, distributed computing systems are expected to play a key role in this direction, as the deployment of advanced ML algorithms as well as the support of highly demanding computational applications, such as blockchain technology and encryption [62], cannot be fulfilled by lightweight IoT devices.
- The implementation of the zero-trust context. To this end, constant authentication of all involved devices takes place, which might significantly increase signaling burden in the network.
- When FL is employed for faster ML training times as well as for privacy protection, a key issue that may rise is non identical data distribution and severe heterogeneity of the produced datasets (data heterogeneity). This is especially the case in large scale network orientations with diverse elements. In this case, either subsets of training nodes are formulated, or TL is employed to further improve ML training latency [63].
- Different policy configurations in various network segments: As stated in the corresponding section, various network and cloud/edge providers may coexist in the computing cloud continuum. In this case, different access and usage policies may pose significant difficulties in proper resource management.
- As the concept of computing continuum spans across IEC environments, the choice among containerization and virtualization is a challenging debate. To this end, each technology has certain advantages/disadvantages which should be carefully examined, as previously mentioned. For example, although virtualized environments provide isolation and security which are extremely important in edge applications, they introduce significant overhead which can have an impact on the performance of lightweight devices. On the other hand, containers, while more resource-efficient, may pose challenges related to security and orchestration in diverse and distributed edge environments.

Based on the above discussion, a high-level view of a proposed architectural approach is depicted in Figure 6. To this end, various key players can be identified, such as the end user, the network provider, the cloud provider, the edge computing platform provider, the IoT provider, the application developer, and the application integrator. The different roles are analyzed in more detail below:

- Network Provider (NP): The NP is providing the network and connectivity resources that allows the interconnection of cloud with near edge and far edge locations as well as the provisioning of the required resources supporting gateways and remote devices connectivity. Within the cloud continuum there can be multiple NPs depending on the footprint of the infrastructure and the administrative domains.

 doi:10.20944/preprints202512.0281.v1

- Cloud Provider (CP): The CP is provisioning the cloud resources responsible for hosting the application components. Commonly, the CP operates on large cloud infrastructures (e.g., Hyper scalars), providing points of presence (PoPs) of local interest for allowing fast connectivity, low latency, load balancing and close to the devices resource availability.
- Edge Computing Platform Provider (ECPP): Similarly, the ECPP is providing cloud resources at the edge (near or far) of the infrastructure, capable of hosting less resource demanding application's components coupled with specific hardware (HW) acceleration capabilities suitable for AI/ML workloads. It is assumed that the ECPP infrastructure topology allows for reaching large and/or dense IoT deployments.
- IoT Provider (IoTP): IoT provider is the actor providing the IoT infrastructure that is being deployed across the continuum. This infrastructure may include devices that allow deployment of continuum controllers or/and agents. Moreover, in the case that the capability to deploy the continuum is restricted either due to processing resources limitations or because of access to the HW device OS, appropriate APIs are exploited. The IoTP through the continuum is gaining the ability to open the infrastructure to multiple vertical applications, since all operate on the common continuum software.
- The Application Developer (AppDev) and the Application Integrator (AppInt) can be seen as distinguishing roles played by the same actor or different, depending on the complexity of the ecosystem. The first one is developing application components, enhancing functionality and operation. The latter one is integrating application components that may arrive even from different developers, so that a full-blown application is created and modelled/described in a compatible to the continuum model. In this context the AppInt is experienced with the presented data model, descriptor, and operation specificities. Consequently, the AppDev depends on the Application Integrator to formulate the application descriptors in a way that is comprehensible by the continuum in order to be deployed over an instance.

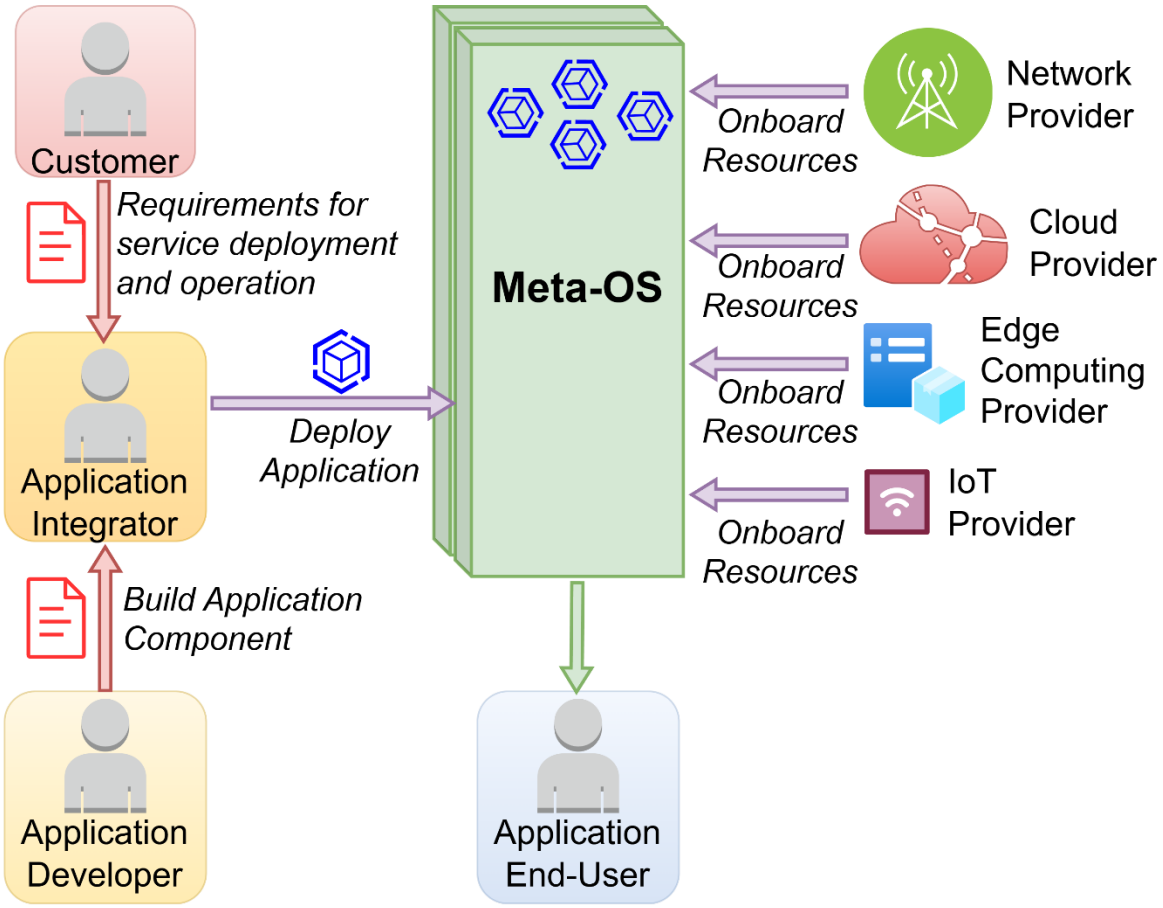

Figure 6. High-level schema of the proposed Meta-OS-enabled computing continuum framework.

 doi:10.20944/preprints202512.0281.v1

Hence, as it becomes apparent from the previous discussion, the computing continuum should provide a unified access mechanism to all the aforementioned key players. In the same context, as previously mentioned, a variety of ML models should be trained and updated, either for resource optimization or for threat mitigation. In parallel, security by design should be also supported. Hence, three main modules can be identified, and in particular the Data Management Module (DMM), the Intelligence Module (IM) and the Security Module (SM). DMM is responsible for managing all data required and exchanged in the continuum, as well as the efficient execution of data-based applications and services used in the continuum. Its main functionalities include: a) Data distribution across the continuum, taking advantage of the entire available infrastructure, b) Smart data placement and dynamic adaptation to changes in the infrastructure during operation: devices joining or leaving, reorganizations, etc., c) Seamless access to data in the continuum, regardless of the location (device or cloud) or nature of resource (in motion or at-rest), by providing an integrated data platform spanning the whole continuum and d) Minimization of data transfers to improve performance and trust, by exploiting near-data processing in various types of devices.

The IM provides the functionalities to train, test, use, maintain and update analytics and ML models in the continuum, with the goal of supporting and augmenting the operations and performance of the security and privacy modules by considering specific policies in the use of data and models, with special emphasis on trustworthiness including:

- Intelligence Layer Coordination: Coordination enables optimization and predictive analytics and ML models and its use across the continuum. This will include policies for the use, share and update of models across the edge-cloud continuum, including FL strategies.
- Data Processing: Data processing and storage in formats and databases optimized for the application of analytics tasks depending on the resources available of the hosting device in the continuum.
- AI Analytics: A library of optimized ML algorithms for training and testing of predictive and optimization models, including deep learning, adaptive machine learning and reinforcement learning libraries optimized to operate in constrained devices.
- AI Models Marketplace: A collection of pre-trained analytics and ML models to be reused, updated, refined (e.g., TL) and combined to foster the application of new AI techniques in the different layers of the computing continuum meta-OS. To this end, a challenging task is to provide the functionality to train and compress these models for operation in constrained devices (e.g., pruning unused branches in trees or simplifying NN architectures).
- Trustworthy AI: Provide specific algorithms to analyze the datasets and develop models conforming to policies for privacy and trustworthiness. Functionality for models to be trained in a FL fashion to ensure data protection in datasets containing user-specific data will be provided as well as explainable AI algorithms to provide reassurance of output of models to the different layers of the continuum.

Finally, the SM provides several related functionalities, such as i) Federated Identity Management; ii) Authentication, Authorization and Audit capabilities; iii) Detection of security issues and mitigation mechanisms (e.g. self-healing); iv) Support for compliance frameworks; v) Trust and privacy.

5. Potential Use Cases

In this subsection various potential use cases are presented, that could be leveraged from the computing continuum and cloud operating systems. These include predictive maintenance in industrial 4.0 applications, load forecasting, smart cities as well as critical infrastructure monitoring. For each use case, a reference architecture is discussed along with signaling requirements.

5.1. Predictive Maintenance in Industrial 4.0 Scenarios

A challenging use case is the predictive maintenance in advanced industrial 4.0 scenarios as well as the provision of immediate responses in latency critical applications. To this end, various IoT

 doi:10.20944/preprints202512.0281.v1

devices are placed in key components of the manufacturing process that constantly collect and process data. These data are send to an edge server that is located in the premises of the industry, as shown in Figure 1. To this end, the interconnection of a vast number of heterogeneous hardware components on one hand and data analysis for effective ML training on the other hand can be made feasible only via the computing continuum. In this case, data analysis targets two actions: a) predictive maintenance of specific components and b) immediate termination of a process, in case this is crucial. For example, in a wind park it is critical for this termination to happen in a predefined time frame, especially in the case of severe wind flows that can damage the machine. In the same context, these edge servers that collect local data can train ML models, as previously mentioned. However, in the case of similar industrial premises, on site edge servers can locally train an ML model, which can be aggregated in a FL fashion way after collecting all parameters from all premises. Although FL ensures privacy by design since only model parameters are exchanged, communication among the premises can be leveraged with the use of private networks [64].

5.2. Load Forecasting in Smart Grid Environments

In load forecasting in the smart grid energy sector the goal is to collect data from various IoT sensors spread across the grid topology and perform accurate load forecasting. These sensors can be placed in production units, renewable energy sources, as well as in households. The aim is to periodically send data to edge servers that collect them and perform accurate load forecasting. As in the previous scenario of predictive maintenance, the goal is to securely interconnect a vast number of interconnected devices that can be spread over large geographical areas. In advanced scenarios, household energy consumption can be measured via IoT measurement devices where with the use of appropriate applications a user can be informed on the actual amount of data under consumption as well as on the predicted data in predefined time intervals. Depending on latency tolerance, ML model training can take place either on local edge servers or in the cloud domain, especially in cases of long-term production planning.

A typical use case for example is depicted in Figure 7, where concentrators collect data generated from smart meters in households. In the operation center, proper IoT data are collected from various modules, such as the geographical information system (GIS) that matches consumed energy with specific households, the data management system (DMS) for load forecasting, the consumer information system (CIS) that provides billing information as well as the operational management system (OMS) that informs the central management system for potential outages.

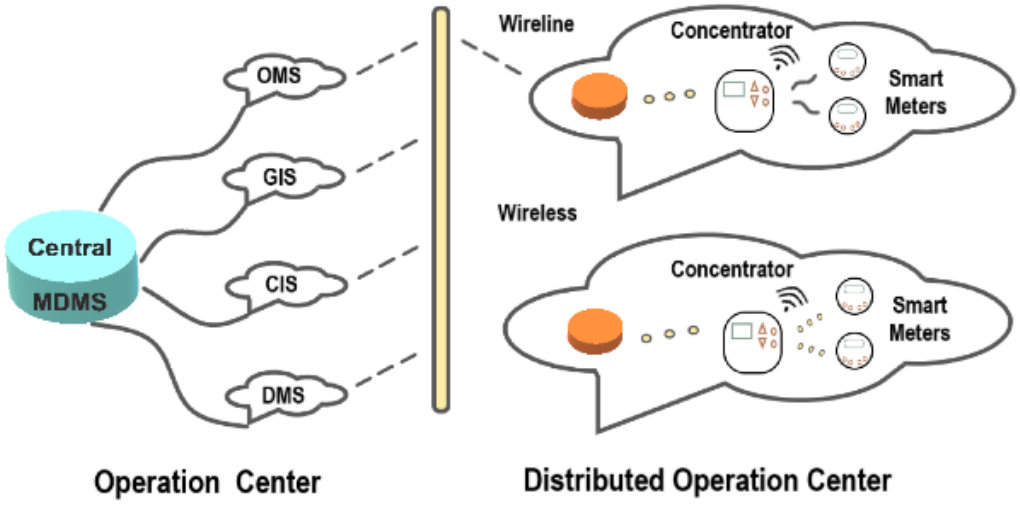

Figure 7. A dispersed communication structural design for Smart Grid based on IoT.

5.3. Smart Cities

 doi:10.20944/preprints202512.0281.v1

In the concept of smart cities, the goal is to place various IoT sensors and measure key performance metrics, such as traffic, air quality, people density, etc [65]. Hence, data generated from a variety of sensors should be properly collected to optimize various parameters directly related to the well-being of citizens, such as the time of arrival of transportation, management of traffic in roads, light density, etc. This concept is also applied in smart buildings, where various operations such as central heating and cooling, air quality, etc. are managed by on site edge servers [66]. As it becomes apparent from the above, a full deployment of the smart city concept presumes the integration of multiple IoT heterogeneous sensors. Hence, data management, communication procedures as well as data integration for efficient ML model training can be quite challenging tasks. To this end, a full layered approach as the one presented in Figure 1 would be the best choice for this scenario. Such an approach can also leverage the deployment of advanced services and applications in 6G scenarios within smart cities, such as autonomous driving.

5.4. Infrastructure Monitoring

In this use case scenario, various IoT sensors are deployed over large scale infrastructures to collect data and leverage predictive maintenance. In railway lines for example, the massive deployment of sensors along different parts of the infrastructure is essential for the optimization and improvement of service and safety. The increasing number of sensors and its specific, and typically siloed solutions, present an increasing complexity related to the management and operations of such solutions.

Today, the railway monitoring process to improve the maintenance cycle is basic, and for most railway operators it is done preventively (once every fixed period) through a special train with sensors on its wheels which runs through the whole rail system. This special train can measure several key parameters of the railway system, such as the height difference and width between two lines, and thus identify where, potentially, corrections in the lines are needed. However, this measurement is only taken every once or twice a year; in the remaining months, nobody knows what happens (only physical inspections are available: very costly and uncommon), and moreover, there is no established procedure to evaluate the cost-effectiveness of the actions taken to address the identified rail line issues. In this context, digital technology, such as IoT, aims to minimize the monitoring and maintenance costs by gaining knowledge of the status of key aspects of the railway infrastructure in real-time: rail tracks levelling, tensions, and slope, surrounding areas settlements and falling elements, catenaries maintenance, cyber processes monitoring, etc.

Hence, the main challenge to be addressed by this use case is related to the continuous monitoring of critical infrastructure on rail tracks to ensure safety and improve maintenance activities. In the same context, energy-efficient solutions for low-power IoT devices are required to guarantee safety operation monitoring in real time while ensuring a very long lifetime of the deployed technology in remote locations. The aforementioned concept can be applied in additional large-scale infrastructures as well. Two typical examples include large hydroelectric stations, where various sensors are deployed over the topology to measure key performance indicators, (e.g. water flow, resistance of the barrier, water quality, etc) as well as in large bridge infrastructures. In the latter case, cracks or malfunctionalities throughout the construction can be easily identified.

A schematic overview of data exchange for various applications in the meta-OS computing continuum is shown in Figure 8. To this end, multiple IoT gateways gather related information from the physical sources and forward it to the continuum instances. For ease of abstraction, the DMM, AI/ML as well as the SM can be placed in an arbitrary module of the continuum, as introduced in Figure 1. Once data is received by the DMM, both the SM as well as the IM can process this information and either update the corresponding ML models or enforce threat detection and privacy policies. In this context, the compliance enforcement module will enable the detection of compliance problems and enforce infrastructural changes in order to enhance compliance based on the chosen target compliance framework. Privacy module will provide a set of primitives that could be used for data transformation, such as anonymisation, and encryption. The anomaly detection module either

 doi:10.20944/preprints202512.0281.v1

receives updated ML models from the IM for threat detection or forwards corresponding data in cases of zero-day attacks.

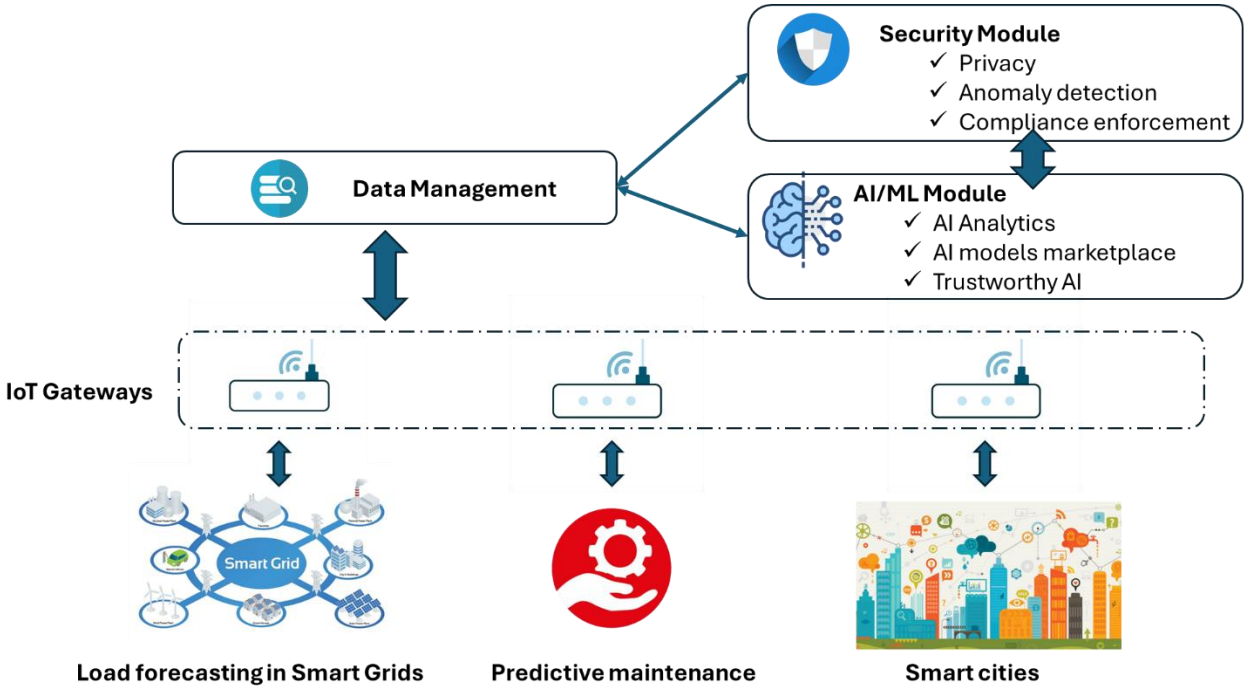

Figure 8. Use cases for interactions and data exchange in the meta-OS-enabled and AI-assisted computing continuum.

6. Conclusions

In this article all recent technological developments in the area of meta – OSs in the computing continuum were analyzed, with emphasis on the support of advanced services and applications. In the same context, several open issues and limitations were identified as well. As it becomes apparent, various key enabling technologies will support this context, such as advanced machine learning algorithms that properly collect data and perform large scale distributed optimization, as well as efficient and lightweight security mechanisms. However, as it became apparent from the discussion in this article, all adopted solutions should be based on open access frameworks, to facilitate interoperability of the connected devices and leverage scalability. In the same context, coexistence with the 6G networks is also a challenging issue, as IoT, edge and cloud devices should be in the position to support advanced services and applications.

Hence, a cutting-edge research effort lies in the deployment of advanced ML approaches that can rapidly adapt to varying network conditions, leverage green computing calculations and at the same time minimize intent creation times for various threats. In this context, a high-level view of a proposed architectural approach was discussed as well, that facilitates the entry and communication of various entities of the continuum and at the same time leverages the creation and storage of advanced ML algorithms to be adopted per case.

Author Contributions: Conceptualization, P.G. and A.G.; methodology, P.G.; software, N.N.; validation, P.T., L.S., V.N., and G.P.; formal analysis, L.S. and V.N.; investigation, N.N.; resources, P.G.; data curation, P.G.; writing—original draft preparation, P.G.; writing—review and editing, A.G., V.N. and G.P.; visualization, N.N. and A.G.; supervision, P.G. and P.T.; project administration, P.G. and P.T. All authors have read and agreed to the published version of the manuscript.

 doi:10.20944/preprints202512.0281.v1

Funding: This work was partially supported by the project «Towards a functional continuum operating system (ICOS)» funded by the European Commission (Project code/Grant Number: 101070177, call for proposal: HORIZON-CL4-2021-DATA-01, funded under HE|HORIZON-RIA\HORIZON-AG).

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

5G	Fifth Generation
6G	Sixth Generation
6GCC	6G Computing Continuum (6GCC)
AI	Artificial Intelligence
AIoT	Artificial Intelligence of Things (AIoT)
AP	Access Point
API	Application Programming Interface
AppDev	Application Developer
AppInt	Application Integrator
CEC	Cloud Edge Continuum
CIS	Customer Information System
CP	Cloud Provider
DCS	Distributed Computing System
DMM	Data Management Module
DMS	Data Management System
DRL	Deep Reinforcement Learning
ECPP	Edge Cloud Platform Provider
EU	European Union
GIS	Geographical Information System
FL	Federated Learning
HW	Hardware
IM	Intelligence Module
IoT	Internet of Things
IoTinuum	IoT Computing Continuum
IoTP	IoT Provider
IEC	IoT Edge Cloud
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NFV	Network Function Virtualization
NN	Neural Network
NP	Network Provider
OS	Operating System
RL	Reinforcement Learning
PaaS	Platform as a Service
PoP	Point of Presence
PUF	Physical Unclonable Function
QoS	Quality of Service
SaS	Security as a Service
SBA	Service Based Architecture
SDN	Software Defined Networking
SDS	Self-Distribution Systems
TL	Transfer Learning

 doi:10.20944/preprints202512.0281.v1

References

1. Abdulhussain, S.H.; Mahmmod, B.M.; Alwhelat, A.; Shehada, D.; Shihab, Z.I.; Mohammed, H.J.; Abdulameer, T.H.; Alsabah, M.; Fadel, M.H.; Ali, S.K.; et al. A Comprehensive Review of Sensor Technologies in IoT: Technical Aspects, Challenges, and Future Directions. *Computers* **2025**, 14, 342. https://doi.org/10.3390/computers14080342.
2. Adam, M.; Hammoudeh, M.; Alrawashdeh, R.; Alsulaimy, B. A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems. *IEEE Access* **2024**, vol. 12, pp. 57128-57149, doi: 10.1109/ACCESS.2024.3382709.
3. Behnke, I; Austad, H. Real-Time Performance of Industrial IoT Communication Technologies: A Review. *IEEE Internet of Things Journal* **2024**, 11(5), 7399-7410, doi: 10.1109/JIOT.2023.3332507.
4. Folgado, F.J.; Calderón, D.; González, I.; Calderón, A.J. Review of Industry 4.0 from the Perspective of Automation and Supervision Systems: Definitions, Architectures and Recent Trends. *Electronics* **2024**, 13, 782. https://doi.org/10.3390/electronics13040782.
5. Gkonis, P.; Giannopoulos, A.; Trakadas, P.; Masip-Bruin, X.; D'Andria, F. A Survey on IoT-Edge-Cloud Continuum Systems: Status, Challenges, Use Cases, and Open Issues. *Future Internet* **2023**, 15, 383. https://doi.org/10.3390/fi15120383.
6. Crespo-Aguado, M.; Lozano, R.; Hernandez-Gobertti, F.; Molner, N.; Gomez-Barquero, D. Flexible Hyper-Distributed IoT–Edge–Cloud Platform for Real-Time Digital Twin Applications on 6G-Intended Testbeds for Logistics and Industry. *Future Internet* **2024**, 16, 431. https://doi.org/10.3390/fi16110431.
7. Masip-Bruin, X.; Marín-Tordera, E.; Sánchez-López, S.; Garcia, J.; Jukan, A.; Juan Ferrer, A.; Queralt, A.; Salis, A.; Bartoli, A.; Cankar, M.; et al. Managing the Cloud Continuum: Lessons Learnt from a Real Fog-to-Cloud Deployment. *Sensors* **2021**, 21, 2974. https://doi.org/10.3390/s21092974.
8. Kaftantzis, N.; Kogias, D.G.; Patrikakis, C.Z. Exploring the Impact of Resource Management Strategies on Simulated Edge Cloud Performance: An Experimental Study. *Network* **2024**, 4, 498-522. https://doi.org/10.3390/network4040025.
9. Almutairi, M.; Sheldon, F.T. IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. *Electronics* **2025**, 14, 1394. https://doi.org/10.3390/electronics14071394.
10. Ficili, I.; Giacobbe, M.; Tricomi, G.; Puliafito, A. From Sensors to Data Intelligence: Leveraging IoT, Cloud, and Edge Computing with AI. *Sensors* **2025**, 25, 1763. https://doi.org/10.3390/s25061763.
11. Cajas Ordóñez, S.A.; Samanta, J.; Suárez-Cetrulo, A.L.; Carbajo, R.S. Intelligent Edge Computing and Machine Learning: A Survey of Optimization and Applications. *Future Internet* **2025**, 17, 417. https://doi.org/10.3390/fi17090417.
12. Elhanashi, A.; Dini, P.; Saponara, S.; Zheng, Q. Advancements in TinyML: Applications, Limitations, and Impact on IoT Devices. *Electronics* **2024**, 13, 3562. https://doi.org/10.3390/electronics13173562.
13. Vaño, R.; Lacalle, I.; Sowiński, P.; S-Julián, R.; Palau, C.E. Cloud-Native Workload Orchestration at the Edge: A Deployment Review and Future Directions. *Sensors* **2023**, 23, 2215. https://doi.org/10.3390/s23042215.
14. The Kube Edge, available online at: https://kubeedge.io/.
15. Prangon, N.F.; Wu, J. AI and Computing Horizons: Cloud and Edge in the Modern Era. *J. Sens. Actuator Netw*. **2024**, 13, 44. https://doi.org/10.3390/jsan13040044.
16. Donta, P.K.; Murturi, I.; Casamayor Pujol, V.; Sedlak, B.; Dustdar, S. Exploring the Potential of Distributed Computing Continuum Systems. *Computers* **2023**, 12, 198. https://doi.org/10.3390/computers12100198.
17. Bittencourt, L. F.; Rodrigues-Filho, R.; Spillner, J.; De Turck (UGent), F.; Pereira dos Santos (UGent), J. P.; da Fonseca, N. L. S.; Rana, O.; Parashar, M.; Foster, I. The computing continuum: past, present, and future. *Computer Science Review*, vol. 58, Nov. **2025**, 100782, https://doi.org/10.1016/j.cosrev.2025.100782.
18. Kazi, B.U.; Islam, M.K.; Siddiqui, M.M.H.; Jaseemuddin, M. A Survey on Software Defined Network-Enabled Edge Cloud Networks: Challenges and Future Research Directions. *Network* **2025**, 5, 16. https://doi.org/10.3390/network5020016.
19. Giannopoulos, A.; Paralikas, I.; Spantideas, S.; Trakadas, P. COOLER: Cooperative Computation Offloading in Edge-Cloud Continuum Under Latency Constraints via Multi-Agent Deep Reinforcement

 doi:10.20944/preprints202512.0281.v1

Learning. In *2024 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS)* **2024**, *pp. 9-16*. DOI: 10.1109/ICCNS62192.2024.10776151

20. Ros, S.; Ryoo, I.; Kim, S. DRL-Driven Intelligent SFC Deployment in MEC Workload for Dynamic IoT Networks. *Sensors* **2025**, 25, 4257. https://doi.org/10.3390/s25144257.
21. Liberti, F.; Berardi, D.; Martini, B. Federated Learning in Dynamic and Heterogeneous Environments: Advantages, Performances, and Privacy Problems. *Appl. Sci.* **2024**, 14, 8490. https://doi.org/10.3390/app14188490.
22. Dawood, M.; Tu, S.; Xiao, C.; Alasmary, H.; Waqas, M.; Rehman, S.U. Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry* **2023**, 15, 1981. https://doi.org/10.3390/sym15111981.
23. Sheikh, A.M.; Islam, M.R.; Habaebi, M.H.; Zabidi, S.A.; Bin Najeeb, A.R.; Kabbani, A. A Survey on Edge Computing (EC) Security Challenges: Classification, Threats, and Mitigation Strategies. *Future Internet* **2025**, 17, 175. https://doi.org/10.3390/fi17040175.
24. Tripi, G.; Iacobelli, A.; Rinieri, L.; Prandini, M. Security and Trust in the 6G Era: Risks and Mitigations. *Electronics* **2024**, *13*, 2162. https://doi.org/10.3390/electronics13112162.
25. Kazmi, S.H.A.; Hassan, R.; Qamar, F.; Nisar, K.; Ibrahim, A.A.A. Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions. *Symmetry* **2023**, 15, 1147. https://doi.org/10.3390/sym15061147.
26. Bast, C.; Yeh, K.-H. Emerging Authentication Technologies for Zero Trust on the Internet of Things. *Symmetry* **2024**, 16, 993. https://doi.org/10.3390/sym16080993.
27. Chataut, R.; Nankya, M.; Akl, R. 6G Networks and the AI Revolution—Exploring Technologies, Applications, and Emerging Challenges. *Sensors* **2024**, 24, 1888. https://doi.org/10.3390/s24061888.
28. Salameh, A.I.; El Tarhuni, M. From 5G to 6G—Challenges, Technologies, and Applications. *Future Interne*t **2022**, 14, 117. https://doi.org/10.3390/fi14040117.
29. Adeogun, R.; Berardinelli, G.; Mogensen, P.E.; Rodriguez, I.; Razzaghpour, M. Towards 6G in-X subnetworks with sub-millisecond communication cycles and extreme reliability. *IEEE Access* **2020**, *8*, 110172–110188. https://doi.org/10.1109/ACCESS.2020.3001625.
30. Berardinelli, G.; Adeogun, R. Hybrid radio resource management for 6G subnetwork crowds. *IEEE Commun. Mag*. **2023**, *61*, 148–154. https://doi.org/10.1109/MCOM.001.2200360.
31. Corici, M. – I. et al. Organic 6G Networks: Vision, Requirements, and Research Approaches," *IEEE Access* **2023**, vol. 11, pp. 70698-70715, 2023, doi: 10.1109/ACCESS.2023.3293055.
32. Judvaitis, J.; Blumbergs, E.; Arzovs, A.; Mackus, A.I.; Balass, R.; Selavo, L. A Set of Tools and Data Management Framework for the IoT–Edge–Cloud Continuum. *Appl. Syst. Innov*. **2024**, 7, 130. https://doi.org/10.3390/asi7060130.
33. Karagiannis, V. Data Sovereignty and Compliance in the Computing Continuum. **2024** *11th International Conference on Future Internet of Things and Cloud* (*FiCloud*), Vienna, Austria, 123-130, doi: 10.1109/FiCloud62933.2024.00027.
34. Nedoshivina, L.; Levacher, K.; Fraser, K.; Halimi, A.; Braghin, B. AI-driven Workload Management in Meta OS. *Proceedings of the 1st International Workshop on MetaOS for the Cloud-Edge-IoT Continuum* (MECC **2024**). *Association for Computing Machinery*, New York, NY, USA, 14–20. https://doi.org/10.1145/3642975.3678963.
35. The FLUIDOS project, https://fluidos.eu/.
36. Verginadis, Y.; et al. NebulOuS: A Meta-Operating System with Cloud Continuum Brokerage Capabilities. *Eighth International Conference on Fog and Mobile Edge Computing* (*FMEC*), Tartu, Estonia, **2023**, pp. 254-261, doi: 10.1109/FMEC59375.2023.10306090.
37. The NebulOus project, https://nebulouscloud.eu/.
38. NEMO: Building the Next Generation Meta Operating System
39. The NEMO project, https://meta-os.eu/.
40. Kamienski, C.; Zyrianoff, I.; Bittencourt, L. F.; Di Felice, M. IoTinuum: The IoT Computing Continuum, *2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things* (*DCOSS-IoT*), Abu Dhabi, United Arab Emirates, **2024**, pp. 732-739, doi: 10.1109/DCOSS-IoT61029.2024.00112.

 doi:10.20944/preprints202512.0281.v1

41. Tärneberg, W. et al. The 6G Computing Continuum (6GCC): Meeting the 6G computing challenges. *1st International Conference on 6G Networking* (*6GNet*), Paris, France, **2022**, pp. 1-5, doi: 10.1109/6GNet54646.2022.9830459.
42. Trakadas, P.; Masip-Bruin, X.; Facca, F.M.; Spantideas, S.T.; Giannopoulos, A.E.; Kapsalis, N.C.; Martins, R.; Bosani, E.; Ramon, J.; Prats, R.G.; et al. A Reference Architecture for Cloud–Edge Meta-Operating Systems Enabling Cross-Domain, Data-Intensive, ML-Assisted Applications: Architectural Overview and Key Concepts. Sensors **2022**, 22, 9003. https://doi.org/10.3390/s22229003.
43. Giannopoulos, A. E.; Paralikas, I.; Spantideas, S. T.; Trakadas, P. HOODIE: Hybrid Computation Offloading via Distributed Deep Reinforcement Learning in Delay-Aware Cloud-Edge Continuum. *IEEE Open Journal of the Communications Society* **2024**, 5, 7818-7841, doi: 10.1109/OJCOMS.2024.3514456.
44. Skianis, K.; Giannopoulos, A.; Gkonis, P.; Trakadas, P. Data Aging Matters: Federated Learning-Based Consumption Prediction in Smart Homes via Age-Based Model Weighting. Electronics 2023, 12, 3054. https://doi.org/10.3390/electronics12143054.
45. Garcia, J.; Masip-Bruin, X.; Giannopoulos, A.; Trakadas, P.; Ordoñez, S. A. C.; Samanta, J.; ... & D'Andria, F. ICOS: An Intelligent MetaOS for the Continuum. In *Proceedings of the 2nd International Workshop on MetaOS for the Cloud-Edge-IoT Continuum* (pp. 53-59) **2025**. https://doi.org/10.1145/3721889.3721929
46. Filho, R. R. et al. A Self-Distributing System Framework for the Computing Continuum. *32nd International Conference on Computer Communications and Networks* (*ICCCN*), Honolulu, HI, USA, **2023**, pp. 1-10, doi: 10.1109/ICCCN58024.2023.10230110.
47. Rahman, A. B.; Charatsaris, P.; Tsiropoulou, E. E.; Papavassiliou, S. Symbiotic Resource Pricing in the Computing Continuum Era. *IEEE Transactions on Mobile Computing* **2025**, 24(7), 6474-6487, doi: 10.1109/TMC.2025.3542017.
48. Sturley, H.; Fournier, A.; Salcedo-Navarro, A.; Garcia-Pineda, M.; Segura-Garcia, J. Virtualization vs. Containerization, a Comparative Approach for Application Deployment in the Computing Continuum Focused on the Edge. *Future Internet* **2024**, 16, 427. https://doi.org/10.3390/fi16110427.
49. Roumeliotis, A.J.; Myritzis, E.; Kosmatos, E.; Katsaros, K.V.; Amditis, A.J. Multi-Area, Multi-Service and Multi-Tier Edge-Cloud Continuum Planning. *Sensors* **2025**, 25, 3949. https://doi.org/10.3390/s25133949.
50. Al-Dulaimy, A. The computing continuum: From IoT to the cloud, Internet of Things, vol. 27, **2024**, 101272, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2024.101272 (https://www.sciencedirect.com/science/article/pii/S2542660524002130).
51. Rossini, R. et al. Open Source in NExt Generation Meta Operating Systems (NEMO). *2024 9th International Conference on Smart and Sustainable Technologies* (*SpliTech*), Bol and Split, Croatia, **2024**, pp. 1-5, doi: 10.23919/SpliTech61897.2024.10612369.
52. Barbareschi, M.; Casola, V.; and D. Lombardi. Ensuring End-to-End Security in Computing Continuum Exploiting Physical Unclonable Functions. **2023** *IEEE International Conference on Cloud Computing Technology and Science* (*CloudCom*), Naples, Italy, 2023, pp. 273-278, doi: 10.1109/CloudCom59040.2023.00051.
53. Sheikh, A.M.; Islam, M.R.; Habaebi, M.H.; Zabidi, S.A.; Bin Najeeb, A.R.; Kabbani, A. Integrating Physical Unclonable Functions with Machine Learning for the Authentication of Edge Devices in IoT Networks. *Future Internet* **2025**, 17, 275. https://doi.org/10.3390/fi17070275.
54. Chef Software DevOps Automation Solutions | Chef. [Online]. Available: https://www.chef.io/.
55. Damian, A. I. et al., Ratio1 meta-OS - decentralized MLOps and beyond. **2025** *25th International Conference on Control Systems and Computer Science* (*CSCS*), Bucharest, Romania, 258-265, doi: 10.1109/CSCS66924.2025.00046.
56. Shah, Q.A.; Shafi, I.; Ahmad, J.; Alfarhood, S.; Safran, M.; Ashraf, I. A Meta Modeling-Based Interoperability and Integration Testing Platform for IoT Systems. *Sensors* **2023**, 23, 8730. https://doi.org/10.3390/s23218730.
57. Petrakis, K.; Agorogiannis, E.; Antonopoulos, G.; Anagnostopoulos, T.; Grigoropoulos, N.; Veroni, E.; Berne, A.; Azaiez, S.; Benomar, Z.; Kakoulidis, H.; et al. Enhancing DevOps Practices in the IoT–Edge–Cloud Continuum: Architecture, Integration, and Software Orchestration Demonstrated in the COGNIFOG Framework. *Software* **2025**, 4, 10. https://doi.org/10.3390/software4020010.
58. The COGNIFOC Project, https://cognifog.eu/.

 doi:10.20944/preprints202512.0281.v1

59. Iman, M.; Arabnia, H.R.; Rasheed, K. A Review of Deep Transfer Learning and Recent Advancements. *Technologies* **2023**, 11, 40. https://doi.org/10.3390/technologies11020040.
60. Heydari, S.; Mahmoud, Q.H. Tiny Machine Learning and On-Device Inference: A Survey of Applications, Challenges, and Future Directions. *Sensors* **2025**, 25, 3191. https://doi.org/10.3390/s25103191.
61. Nomikos, N.; Xylouris, G.; Patsourakis, G.; Nikolakakis, V.; Giannopoulos, A.; Mandilaris, C.; Gkonis, P.; Skianis, C.; Trakadas, P. A Distributed Trustable Framework for AI-Aided Anomaly Detection. *Electronics* **2025**, 14, 410. https://doi.org/10.3390/electronics14030410.
62. Zhao, J.; Zhang, Y.; Jiang, J. Blockchain-Based Distributed Computing Consistency Verification for IoT Mobile Applications. *Appl. Sci.* **2023**, 13, 7762. https://doi.org/10.3390/app13137762.
63. Barona López, L.I.; Borja Saltos, T. Heterogeneity Challenges of Federated Learning for Future Wireless Communication Networks. *J. Sens. Actuator Netw.* **2025**, 14, 37. https://doi.org/10.3390/jsan14020037.
64. Trakadas, P.; Sarakis, L.; Giannopoulos, A.; Spantideas, S.; Capsalis, N.; Gkonis, P.; Karkazis, P.; Rigazzi, G.; Antonopoulos, A.; Cambeiro, M.A.; et al. A Cost-Efficient 5G Non-Public Network Architectural Approach: Key Concepts and Enablers, Building Blocks and Potential Use Cases. *Sensors* **2021**, 21, 5578. https://doi.org/10.3390/s21165578.
65. Lea, R.; Adame, T.; Berne, A.; Azaiez, S. The Internet of Things, Fog, and Cloud Continuum: Integration Challenges and Opportunities for Smart Cities. *Future Internet* **2025**, 17, 281. https://doi.org/10.3390/fi17070281.
66. Ożadowicz, A. Generic IoT for Smart Buildings and Field-Level Automation—Challenges, Threats, Approaches, and Solutions. *Computers* **2024**, 13, 45. https://doi.org/10.3390/computers13020045.