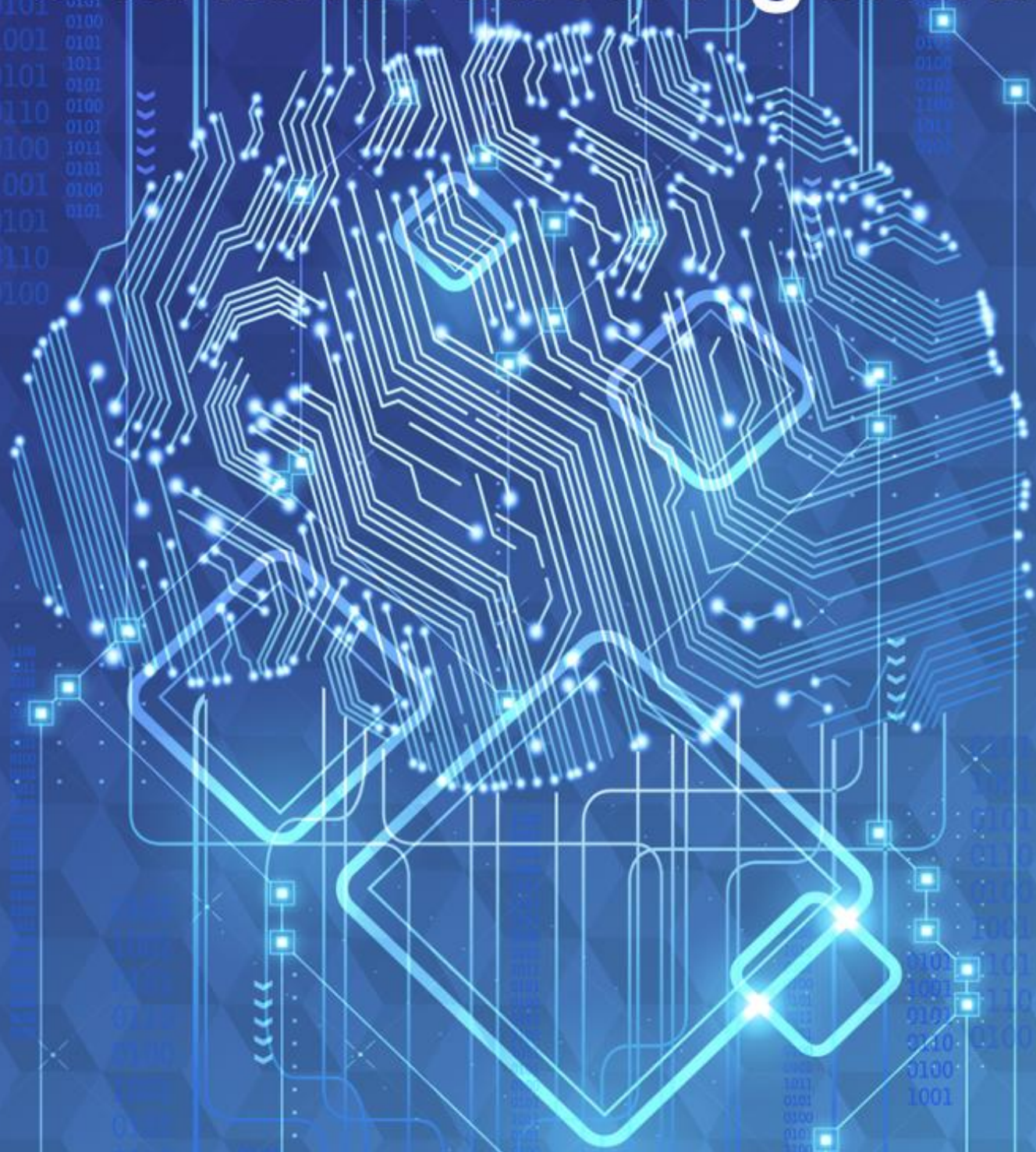
Alliance for IoT and Edge Computing Innovation

AIOTI Strategic Research and Innovation Agenda



Advancing Next-Generation IoT and Edge Computing Research and Innovation

Executive Summary

The Alliance for IoT and Edge Computing Innovation (AIOTI) Strategic Research and Innovation Agenda (SRIA) aims both at identifying key Internet of Things (IoT) and edge computing technologies and applications research priorities and at providing a vision on how the future of the IoT domain will look like, up until the 2030 timeframe.

The AIOTI SRIA is a roadmap (2023-2030) for future IoT and edge computing research and innovation actions in Europe, proposing specific themes, sub-themes, and priorities, which help identifying gaps and areas where research and innovation advancements are most needed.

The identified research priorities form the reference for concrete actions to be implemented in different research programmes by various stakeholders, such as industry, researchers, small-and-medium enterprises, academia, entrepreneurs, the public sector, and the overall society.

The SRIA delivers a direct contribution in aligning with the United Nations Sustainable Development Goals (SDG) needs and the European Green Deal objectives, while developing international cooperation to solve global challenges using IoT and cloud computing technologies.

The research and innovation efforts in IoT and edge computing require to be based on a long-term programming approach that provides continuity across technology and applications efforts over several years. The AIOTI SRIA introduces a mission-oriented research and innovation approach that answers societal and market needs, maintains, and extends industrial leadership, protects the environment, ensures security, privacy, safety, and energy efficiency solutions, while prioritising research and innovation capabilities and education.

The AIOTI SRIA addresses research and innovation priorities for future IoT and edge computing technologies and applications that will drive changes across industrial sectors, the European economy, and society. The priorities include convergence with next-generation Tactile IoT, decentralised and distributed architectures, IoT knowledge-driven edge processing, artificial intelligence (AI) and trustworthiness.

The IoT and edge computing technologies have evolved rapidly in addressing the grand challenge of developing human centred IoT technologies and applications, which require increased communication and coordination amongst policy makers, end-users, and experts in the IoT and edge computing fields.

The extensive use of IoT and edge computing in different industrial sectors and the move from cloud to edge processing must be accompanied by new distributed architectures and end-to-end (E2E) IoT security. The convergence of connectivity, IoT, edge computing, AI, and Distributed Ledger Technologies (DLT) will be essential to next-generation Internet applications and advancements.

The topics presented in the AIOTI SRIA are aligned with the issues addressed by other European partnerships to improve the European IoT ecosystem's sustainability and manage human well-being, particularly for developing safe, secure, and trustworthy IoT and edge computing technologies.

Table of Content

Executive Summary 2

Table of Figures 6

List of Tables 7

List of Acronyms 8

1. Vision, Mission and Objectives 10

2. IoT and Edge Computing Technological Research and Innovation 12

3. IoT and Edge Computing Granularity 16

3.1 Technological developments 16

3.2 Main Trends, Issues and Challenges 19

3.3 Research Priorities Timeline 20

4. IoT Edge and X-Continuum Paradigm 21

4.1 Technological developments 21

4.2 Main Trends, Issues and Challenges 22

4.3 Research Priorities Timeline 23

5. Intelligent Connectivity 24

5.1 Technological developments 24

5.2 Main Trends, Issues and Challenges 25

5.3 Research Priorities Timeline 28

6. Energy-Efficient Intelligent IoT and Edge Computing Systems 29

6.1 Technological developments 29

6.2 Main Trends, Issues and Challenges 30

6.3 Research Priorities Timeline 31

7. Heterogeneous Cognitive Edge IoT Mesh 32

7.1 Technological developments 32

7.2 Main Trends, Issues and Challenges 33

7.3 Research Priorities Timeline 35

8. IoT Digital Twins, Modelling and Simulation Environments 36

8.1 Technological developments 36

8.2 Main Trends, Issues and Challenges 38

8.3 Research Priorities Timeline 38

9. IoT Swarm Systems 39
9.1 Technological developments 39
9.2 Main Trends, Issues and Challenges 40
9.3 Research Priorities Timeline 42
10. Internet of Things Senses 43
10.1 Technological developments 43
10.2 Main Trends, Issues and Challenges 45
10.3 Research Priorities Timeline 46
11. Decentralised and Distributed edge IoT Systems 47
11.1 Technological developments 47
11.2 Main Trends, Issues and Challenges 48
11.3 Research Priorities Timeline 49
12. Federated Learning, Artificial Intelligence technologies and learning for edge IoT Systems 50
12.1 Technological developments 50
12.2 Main Trends, Issues and Challenges 51
12.3 Research Priorities Timeline 53
13. Operating Systems and Orchestration Concepts for edge IoT Systems 54
13.1 Technological developments 54
13.2 Main Trends, Issues and Challenges 55
13.3 Research Priorities Timeline 56
14. Dynamic Programming Tools and Environments for Decentralised and Distributed IoT Systems 57
14.1 Technological developments 57
14.2 Main Trends, Issues and Challenges 57
14.3 Research Priorities Timeline 59
15. Heterogeneous Edge IoT Systems Integration 60
15.1 Technological developments 60
15.2 Main Trends, Issues and Challenges 61
15.3 Research Priorities Timeline 62
16. Edge IoT sectorial and Cross-Sectorial Open Platforms 63
16.1 Technological developments 63
16.2 Main Trends, Issues and Challenges 64
16.3 Research Priorities Timeline 65

17. IoT Verification, Validation and Testing (VV&T) Methods 66
17.1 Technological developments 66
17.2 Main Trends, Issues and Challenges 66
17.3 Research Priorities Timeline 67
18. IoT Trustworthiness and Edge Computing Systems Dependability 68
18.1 Technological developments 68
18.2 Main Trends, Issues and Challenges 69
18.3 Research Priorities Timeline 71
Contributors 72
Acknowledgements 74
About AIOTI 75

Table of Figures

Figure 1 Edge IoT research and innovation topics 12

Figure 2 Edge computing granularity across the computing continuum 17

Figure 3 Edge cloud continuum representation 18

Figure 4 X- continuum paradigm 21

Figure 5 Matter and Thread edge IoT connectivity 27

Figure 6 Edge IoT digital twin technology evolution 37

Figure 7 Internet of things senses 44

Figure 8 Edge IoT system dependability characteristics 68

List of Tables

Table 1 IoT and edge computing research priorities 20

Table 2 IoT edge and X-Continuum research priorities 23

Table 3 Intelligent connectivity research priorities 28

Table 4 Energy-efficient intelligent IoT and edge computing systems research priorities 31

Table 5 Heterogeneous cognitive edge IoT mesh research priorities 35

Table 6 IoT Digital Twins, Modelling and Simulation Environments research priorities 38

Table 7 Swarm systems research priorities 42

Table 8 Internet of things senses research priorities 46

Table 9 Decentralised and distributed edge IoT systems research priorities 49

Table 10 Federated learning and AI for edge IoT systems research priorities 53

Table 11 Operating systems and orchestration concepts for edge IoT systems research priorities 56

Table 12 Dynamic programming tools and environments for edge IoT systems research priorities 59

Table 13 Heterogeneous edge IoT systems integration research priorities 62

Table 14 Edge IoT sectorial and Cross-Sectorial Open Platforms research priorities 65

Table 15 IoT Verification, Validation and Testing Methods research priorities 67

Table 16 IoT Trustworthiness and Edge Computing Systems Dependability research priorities 71

List of Acronyms

AI	Artificial Intelligence
AIOp	Artificial Intelligence Operations
AIOTI	Alliance for IoT and Edge Computing Innovation
AIOTI SRIA	AIOTI Strategic Research and Innovation Agenda
ANDSF	Access Network Discovery and Selection Function
ANN	Artificial Neural Network
API	Application Programming Interface
AR	Augmented Reality
ASIC	Application-Specific Integrated Circuit
ASSP	Application-Specific Standard Product
AV	Audio Video
BS	Base Station
CBOR	Concise Binary Object Representation
CN	Cognitive Network
CPU	Central Processing Unit
D2D	Device-Device
DL	Deep Learning
DLT	Distributed Ledger Technologies
DMO	Direct Mode Operation
DSP	Digital Signal Processing
DT	Digital Twin
E2E	End to End
ENISA	European Union Agency for Network and Information Security
FL	Function Level
FPGA	Field-Programmable Gate Array
FW	Firmware
GPU	Graphics Processing Unit
H2H	Host to Host, Human to Human
HE	Horizon Europe
HMI	Human-Machine Interface
HW	Hardware
IaaS	Infrastructure as a Service
ID	Identifiers Definition
IETF OSCORE	Internet Engineering Task Force Object Security for Constrained RESTful Environments
IoT	Internet of Things
IoT DT	IoT Digital Twin
IoTS	Internet of Things Senses
IT/OT	Information/Operation Technology
JSON-LD	JavaScript Object Notation for Linked Data

KPI	Key Performance Indicator ()
LDS	Laser-Direct Structuring
LoRa	Long Range Radio
LPWAN	Low-Power Wide Area Network
M2H	Machine to Human
M2M	Machine to Machine
MEC	Multi-access Edge Computing
ML	Machine Learning
MLOp	Machine Learning Operations
mMTC	Machine Type Communication
MR	Machine Reasoning
NPN	Non-Public-Network
NPU	Network Processing Unit
O-RAN	Open Radio Access Network
OEM	Original Equipment Manufacturer
OS	Operating System
OTA	Over-the-Air
PaaS	Platform as a Service
PCI	Peripheral Component Interconnect
PLC	Programmable Logic Controller
QoI	Quality of Information
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RF	Radio Frequency
RISC-V	reduced Instruction Set Computer principles 5th generation
RU	(Multi-)Resource Unit
SCADA	Supervisory Control and Data Acquisition
SDG	Sustainable Development Goals
SDO	Service Data Objects
SLO	Service Level Objective
SoC	System-on-a-Chip
SRE	Site Reliability Engineers
SRIA	Strategic Research and Innovation Agenda
SW	Software
TPU	Tensor Processing Unit
TSN	Time-Sensitive Networking
VR	Virtual Reality
Wi-Fi	Wireless Fidelity
XAI	Explainable AI
XR	eXtended Reality
VV&T	Verification, Validation and Testing

1. Vision, Mission, and Objectives

The vision of AIOTI is "to lead, promote, bridge and collaborate in IoT and edge computing and other converging technologies research and innovation, standardisation and ecosystem building providing IoT and edge computing deployment for European businesses creating benefits for European society. We co-operate with other global regions to ensure removal of barriers to development of the IoT and edge computing market, while preserving the European values, including privacy and consumer protection".

In this context, the AIOTI mission is "to drive on behalf of our members business, policy, research and innovation development in the IoT and edge computing and other converging technologies across the Digital Value Chain to support digitization in Europe, and competitiveness of Europe".

The AIOTIA SRIA reflects the needs of the European IoT and edge computing community and the members of the AIOTI to achieve the above vision and mission. Contributions from the AIOTI Work Groups (WGs) form the basis of the AIOTI SRIA. This document presents some leading IoT and edge computing challenges the European ecosystem will face in the forthcoming years. It introduces evolving activities that may inspire future research and innovation programmes and calls in the European Research and Innovation Framework Programme Horizon Europe (HE). Cooperation and alignment with the new European partnerships and initiatives is essential in this context.

The vision for the AIOTI SRIA is to foster a dynamic IoT, and edge computing European ecosystem based on heterogeneous technology integration into digital value chains across several industrial sectors.

The AIOTI SRIA mission is to support, enhance and strengthen Europe's IoT and edge computing research and innovation capabilities to advance the digital and green transformation, based on sustainable and trustworthy technologies and applications development.

The structure of the 2023 AIOTI SRIA builds on IoT and edge computing technologies trends. It extends the technologies convergence aims to industrial sector vertical areas, which correspond to the different elements of the IoT/edge continuum architectural stack and to IoT and edge computing applications across the different industrial sectors.

The AIOTI SRIA identifies technological development, key trends, issues, and challenges within different thematic areas related to next-generation IoT and edge computing advancements, while providing several selected research priorities over the 2023-2030 period. The goal is to accelerate the technological developments in these thematic areas to unlock the potential of IoT and edge computing in Europe.

The AIOTI SRIA objectives are to support the IoT and edge computing technologies and applications to evolve into an integrated digital ecosystem, characterised by distributed architectures and mesh topologies for advancing hyperautomation in all-industrial sectors. Leveraging digital technologies aims to transform the industrial sector and to deliver scalable, trustworthy, and dependable IoT and edge computing systems for automated and autonomous applications based on heterogeneous technology integration.

Addressing the IoT and edge computing key challenges presented in the AIOTI SRIA requires increased efficiency, scalability, resilience, and interoperability for the provided IoT and edge computing solutions. At the same time, the cycle of change must be made more efficient and shortened, rapidly identifying the most promising solutions, and promoting new ideas, concepts, and advanced technologies.

The AIOTI SRIA describes some major research and innovation topics that the AIOTI stakeholders have identified and can be used as a basis to define next steps of the various European partnerships and research programmes across Europe.

The AIOTI SRIA is composed of sixteen chapters focusing on the current technology layers and their technical challenges along the IoT/edge continuum. The chapters address the key technology building blocks as essential ingredients for the next generation edge IoT systems. These technology components, as part of integrated advanced heterogenous edge IoT systems, will provide some needed and unique features of future applications across industrial sectors. The intelligent connectivity, mesh networking, AI, digital twins, and software technologies are all part of the IoT edge continuum for implementing edge IoT systems of systems. The addressed topics are an integrated part of the IoT/edge continuum layered architecture to build the capabilities to advance the digital and green transformation in the future for the benefit of the whole society.

The AIOTI SRIA is designed to be application domain and funding programme agnostic and can be utilised as a foundation for different industrial vertical applications and as input to the various cooperative work programmes across Horizon Europe, Digital Europe and the European partnerships.

2. IoT and Edge Computing Technological Research and Innovation

IoT and edge computing research and innovation address IoT/edge continuum distributed architectures, intelligent connectivity, E2E security, heterogenous IoT edge mesh, IoT digital twins, AI, IoT swarm systems, Internet of Things Senses (IoTS), trustworthiness, verification, validation, testing, standardisation, and the convergence of all the above into the Internet of Intelligent Things.

IoT and edge computing will see innovation and broad adoption in consumer and industrial IoT vertical sectors, enabling better security practices and reducing connectivity costs.

The overall topics addressed by the AIOTI SRIA document are illustrated in **Figure 1**.

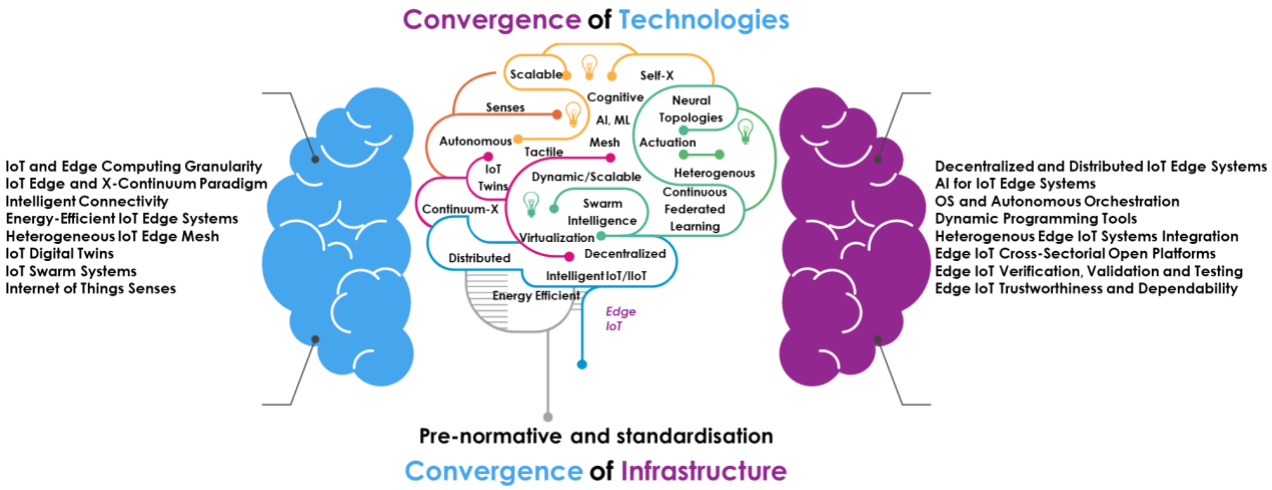


Figure 1 Edge IoT research and innovation topics

The IoT devices, mobile computing units, and fleets of these interconnected devices are evolving, and the information generated and exchanged by these devices grow significantly at the network edge. Consequently, the constraints due to extremely high latency and network bandwidth usage will limit the transfer of these massive volumes of data to the cloud. Using AI processing capabilities at the network edge can unleash the potential of data generated by sensors and devices.

Processing data at the edge brings several benefits, such as reducing latency, needed bandwidth, deployment and equipment costs, power consumption and memory footprint, as well as increasing security and data protection.

The increased computing capabilities at the edge require newly advanced, efficient, and specialised processing architectures, in the mid-long term made of a heterogeneous mix of different computing modules interacting together on demand (Field Programmable Gate Arrays (FPGA), x86-based, ARM-based, neuromorphic-based, Graphic Processing Unit (GPU)-based, AI-based-chips)[1],[2],[3] to improve edge computing performances by several orders of magnitude and drastically reduce power consumption, and costs of maintenance and deployment.

Digital transformation is advancing hyperautomation, which allows for automating the process in the all-industrial sectors. The adoption of hyperautomation aims to streamline processes across the operations using edge processing, IoT, AI, robotic process automation, and other technologies to run with minimum or without human intervention.

Hyperautomation enables the use of multiple tools that allow intelligent automation, including Machine Learning (ML) and connected autonomous IoT systems to scale automation application. The resulting systems are both cross-functional and scalable.

The advancement in edge IoT systems is accelerated by the developments in connectivity mesh that provides local network topologies in which the infrastructure IoT nodes connect directly, dynamically, and non-hierarchically to other nodes and cooperate with them to route efficiently data to and from the networked IoT devices. This topology allows for implementing distributed edge IoT processing capabilities, and the lack of dependency on one node allows for every node to participate in the relay of information.

Mesh networks dynamically self-organise, self-heal, and self-configure, thus drastically reducing installation and maintenance overheads. The ability to self-configure enables the dynamic distribution of edge AI workloads, particularly when a few IoT devices fail, contributing to fault tolerance and reduced maintenance costs. Mesh networking increases the overall range of communication of every command sent back and forth to the objects in the network. This directly translates into an increasingly comprehensive range of possible action for the edge IoT devices.

The IoT mesh networking advantages are the increase in the quality of communications proportionally with the density of nodes and the increase in the distance of communications from the gateway. The deployment topology can optimise the number of devices as each IoT node acts as a router and automatically commissions new nodes within the network space while implementing network auto-repairs.

The evolution of IoT systems from centralised, cloud-based to decentralised and distributed edge-based brings new trends in implementing the concept of cybersecurity mesh developed alongside edge IoT technologies, to provide a holistic approach to network and IoT applications security that integrates different, independent security services into a flexible distributed architecture. Edge AI devices are independently protected using security solutions tailored to their processing capabilities, providing more local control and better overall protection.

[1] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," in IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1657-1681, third quarter 2017, doi: 10.1109/COMST.2017.2705720.

[2] P. Ramachandran, S. Ranganath, M. Bhandaru and S. Tibrewala, "A Survey of AI Enabled Edge Computing for Future Networks," 2021 IEEE 4th 5G World Forum (5GWF), Montreal, QC, Canada, 2021, pp. 459-463, doi: 10.1109/5GWF52925.2021.00087.

[3] F. Shirin Abkenar et al., "A Survey on Mobility of Edge Computing Networks in IoT: State-of-the-Art, Architectures, and Challenges," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2329-2365, Fourth quarter 2022, doi: 10.1109/COMST.2022.3211462.

The design and adoption of potentially new access technologies, in additional to the several ones that already exist at the edge (LoRA, Zigbee, SigFox, Wi-Fi, and Cellular), and of optimized protocols for distributed and device-to-device communications, will be needed to allow for the support of an always increasing heterogeneity of types of devices deployed at the edge.

To that extent, successful alignment within the broad ecosystem of standardization of such technologies and protocols, like the Multi-Access-Edge Computing (MEC) standard driven by ETSI, or other standards from 3GPP and IEEE just to mention a few Standard Developing Organizations (SDOs), will be a key aspect for a successful adoption of forthcoming technologies for the benefit of the broader society. European associations like AIOTI will be instrumental in playing a pivotal role in creating this consensus, thanks to the work done in pre-standards Work Groups like AIOTI Standardization.

Future developments in wireless communication technologies are opening the door for more advanced edge IoT devices and data traffic. The trend accelerates the adoption of edge computing processing in IoT applications, making it easier to process data faster and closer to the data collection and action infrastructure functions, requiring processing enhancements through edge AI. The AI algorithms can leverage ML and more advanced techniques like DL and continuous learning[4], allowing the IoT applications to extract more value from their large volumes of data.

AI is more and more a fundamental ingredient of edge IoT, supporting IoT data analysis in data preparation, discovery, streaming, time series accuracy, predictive and advanced analytics, and real-time localisation and processing.

Edge IoT DT technology will further develop into an edge metaverse by integrating new virtual and soft sensor concepts, thus rapidly becoming an essential technology enabler for needed improvements in several important vertical sectors, e.g., making manufacturing more efficient and profitable. DTs will become an integrated part of the edge industrial IoT solutions using data integration and analysis, mostly needed in interconnected manufacturing processes[5].

The advances in edge processing capabilities require that sensors are increasingly improved with key IoT sensor technology innovations, including increased computing capacity and the ability to detect signals from multiple sensing elements. The increased processing capabilities and edge AI techniques allow the sensors to process signals directly (e.g., validating and interpreting the data, displaying the results, or running specific analytics applications). Edge IoT devices are more and more broadly incorporating AI into their design. They are used for AI inference, allowing decisions to be made immediately and sensitive data to be processed locally thus also increasing security protection and system robustness to external attacks.

The edge IoT devices will make more efficient use of edge computing, as the technology that distributes the processing load and moves it closer to the edge of the network and in the proximity of the sensors that collect data. This will further minimise latency, conserve network bandwidth, securely collect large amounts of data, and process the data closer to the sources, thus allowing for better analysis and insights into local data.

[4] R. Hadsell, et Al., "Embracing Change: Continual Learning in Deep Neural Networks,", Trends in Cognitive Sciences, Volume 24, Issue 12, 2020, https://doi.org/10.1016/j.tics.2020.09.004.

[5] A. Arora and R. Gupta, "A Comparative Study on Application of Artificial Intelligence for Quality Assurance in Manufacturing," *2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2022, pp. 1200-1206, doi: 10.1109/ICIRCA54612.2022.9985522.

Edge computing furthermore makes on-edge device AI more attractive for different applications by leveraging real-time datasets6. This trend will facilitate a balance between the cloud and more distributed edge processing for most IoT services and applications.

This trend will be strengthened by the fact that HW manufacturers are starting to build specific infrastructure for the edge, designed to be more physically rugged and secure. At the same time, security providers offer endpoint security solutions to existing services to prevent data loss, give insights into network health and threat protection, include user control, and that accelerate the adoption and spread of edge computing implementations by IoT applications.

Security issues are becoming increasingly important, and IoT applications will have to ensure security and compliance on various levels, including data encryption, active consent, multiple means of verification and other mechanisms[7]. These enhancements will allow collecting data at the edge legitimately and keep the burden of operations like access, processing, and storage to a minimum, anyway, dictated by the running IoT application.

Energy harvesting and energy efficiency will continue to be IoT edge system design priorities. Once deployed, they will lead to changes in sensor design, AI algorithms, processing, and communication units, making the edge IoT devices more power-efficient by using small ultra-low-powered microcontrollers. This trend will also improve the overall signal-to-noise ratio, by including signal processing components that manage to filter out noise or adding interferences that make the signal processing much more energy efficient.

Another interesting research vector is represented by the integration of different types of soft and virtual sensors into the edge IoT DTs[8]. The soft sensor will implement computational algorithms that estimate the value of a desired quantity based on other existing physical sensors and algorithms/computational models, that infer the value of the measured quantity. The virtual sensors will provide estimated values based on the data from physical sensors, combined with novel algorithms and computational models.

As the mesh wireless technology advances, there will be a shift from the intelligent edge onto the intelligent mesh and security mesh, embedded in the edge architecture allowing the implementation of more responsive edge IoT systems.

.

[6] Dhiraj Joshi; Nirmit Desai; Shyama Prosad Chowdhury; Wei-Han Lee; Luis Bathen; Shiqiang Wang; Dinesh Verma, "AI at the Edge: Challenges, Applications, and Directions," in IoT for Defense and National Security, IEEE, 2023, pp.133-160, doi: 10.1002/9781119892199.ch9.

[7] M. Caprolu, R. Di Pietro, F. Lombardi and S. Raponi, "Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues," 2019 IEEE International Conference on Edge Computing (EDGE), Milan, Italy, 2019, pp. 116-123, doi: 10.1109/EDGE.2019.00035.

[8] L. Cristaldi, A. Ferrero, M. Macchi, A. Mehrafshan and P. Arpaia, "Virtual Sensors: a Tool to Improve Reliability," 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, Roma, Italy, 2020, pp. 142-145, doi: 10.1109/MetroInd4.0IoT48571.2020.9138173.

3. IoT and Edge Computing Granularity

The concept of data processing, analysis and storage using the centralised cloud computing paradigm, comprising of a set of technologies, infrastructure, services, and applications, is no longer aligned with the always increasing demand of cellular, e.g., massive Machine Type Communication (mMTC), services and wireless intelligent connectivity usage scenarios[9]. Such scenarios aim at ensuring that the always growing number of IoT devices connected to the network can operate according to their specification, do not operate under conditions limiting the capabilities, and fulfil the expected Quality of Service (QoS). A new approach is therefore looked for, so to avoid creating silos and issues regarding both connectivity and real-time data processing and storage.

Edge computing provides the mechanisms for distributing data processing and redefines the IoT landscape by moving data processing and analytics at the edge by using AI/ML techniques and ensuring an advanced level of embedded security.

Edge computing allow an effective deployment of real-time applications, considering that the processing is performed close to the data source. It also reduces the order of magnitude of transmitted data, by not transmitting the extensive amount of raw data created by IoT devices, rather just sending smaller amount of data, thanks to storage and local processing capabilities.

Several benefits can be derived by this approach, e.g., a decrease in needed communication bandwidth and data storage requirements, as well as in the data attack surface, thus Improving security, privacy data protection, and finally also reducing the overall energy consumption.

Edge computing solutions are implemented through different deployment forms such as cloudlet[10], dew[11], mobile edge[12], fog computing[13], etc., that have been developed over the last few years.

3.1 Technological developments

Edge computing is defined as a paradigm that can be implemented using different architectures built to support an IoT distributed infrastructure of data processing (signals, image, voice, etc.) with edge IoT devices operating close to the points of collection (data sources) and utilisation. The edge computing distributed paradigm provides computing capabilities to the IoT nodes and devices of the edge of the network (or edge domain) to improve the performance (energy efficiency, latency, etc.), operating cost, security and reliability of applications and services. Edge computing performs data analysis by minimising the distance between IoT nodes and devices and reducing the dependence on centralised resources that serve them while minimising network hops.

[9] B. Raaf et al., "Key technology advancements driving mobile communications from generation to generation", in Intel Technology Journal 18 (1), 2014.

[10] D. Bhatta and L. Mashayekhy, "Physics-Inspired Mobile Cloudlet Placement in Next-Generation Edge Networks," 2022 IEEE International Conference on Edge Computing and Communications (EDGE), Barcelona, Spain, 2022, pp. 159-168, doi: 10.1109/EDGE55608.2022.00031.

[11] Z. S. Ageed, S. R. M. Zeebaree, M. A. M. Sadeeq, R. K. Ibrahim, H. M. Shukur and A. Alkhayyat, "Comprehensive Study of Moving from Grid and Cloud Computing Through Fog and Edge Computing towards Dew Computing," 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), Najaf, Iraq, 2021, pp. 68-74, doi: 10.1109/IICETA51758.2021.9717894.

[12] J. Lee and W. Na, "A Survey on Mobile Edge Computing Architectures for Deep Learning Models," 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2022, pp. 2346-2348, doi: 10.1109/ICTC55196.2022.9952954.

[13] I. Martinez, A. S. Hafid and A. Jarray, "Design, Resource Management, and Evaluation of Fog Computing Systems: A Survey," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2494-2516, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3022699.

IoT edge computing capabilities include a steady operating procedure across different platform infrastructures to deliver processing services to remote IoT devices, application integration, orchestration, and service delivery requirements. The edge computing technologies are meant to properly consider hardware (HW) limitations and cost constraints, to effectively handle limited or intermittent network connections, and to implement methods to satisfy the most diverse requirement sets, e.g., IoT applications requiring low latency or greatly differing in data rates.

For intelligent IoT applications, the edge computing concept is mirrored in the development of different edge computing levels (micro, deep, meta), that incorporate the computing and intelligence continuum from the sensors/actuators, processing units, controllers, gateways, on-premises servers to the interface with multi-access, fog, and cloud computing.

Edge IoT devices and their functions cover the edge computing, communication, and data analytics capabilities, so to make it possible to call such devices smart or intelligent. An edge IoT device is designed around the computing units (CPUs, GPUs/FPGAs, ASICs platforms, AI accelerators/processing), communication network, storage infrastructure and the applications (workloads) that run on it.

The edge domain can scale from a few IoT devices to tens of thousands of IoT devices, distributed in different locations with a unique identity. The IoT devices in the edge computing environment are physically separated and connected using wireless or wired connections in different kinds of topologies, e.g., by using a mesh network[14]. The IoT edge devices can even operate semi-autonomously, especially in the case of sensors spread in remote locations, using remote management administration tools.

The edge devices can be optimised based on different aspects, like processing, memory, energy, connectivity, size, cost. Their performance and capabilities are of course constrained by these parameters.

A description of the micro-, deep- and meta-edge concepts is provided in the following sections and aligned with other European partnerships[15]. The granularity of the edge computing environments is illustrated in **Figure 2**.

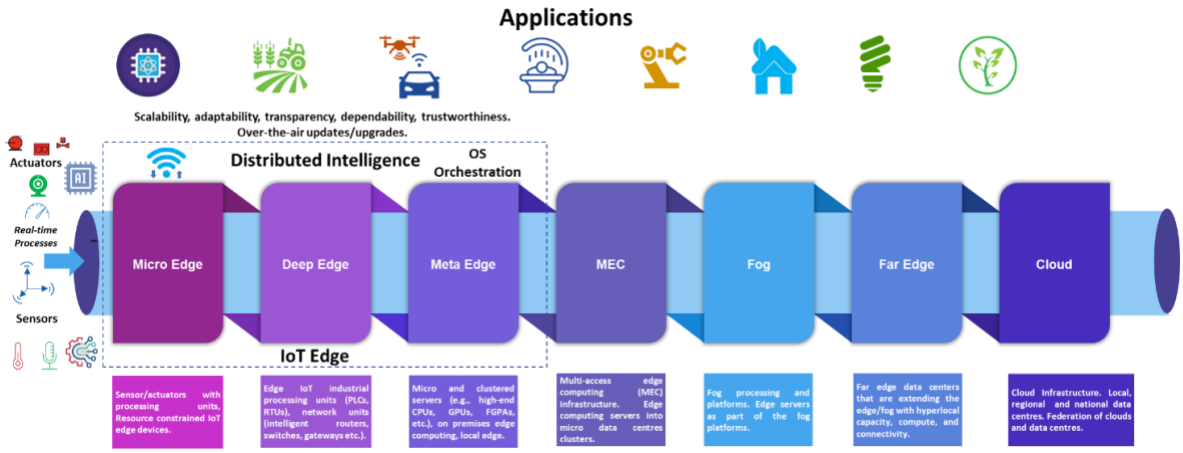


Figure 2 Edge *computing granularity across the computing continuum*

The ***micro-edge*** describes the intelligent sensors, machine vision, and IoT devices that generate insight data and are implemented using microcontrollers built around processors that can well

[14] Karthika K.C, "Wireless mesh network: A survey," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016, pp. 1966-1970, doi: 10.1109/WiSPNET.2016.7566486.

[15] Vermesan, O., Pétrot, F., Coppola, M., Schneider, M. and Höß, A. (Authors). Industrial AI Technologies for Next-Generation Autonomous Operations with Sustainable Performance, in "Intelligent Edge-Embedded Technologies for Digitising Industry" (Chapter 1), River Publishers Series in Communications, June 2022. ISBN: 9788770226110, e-ISBN: 9788770226103. Online at: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788770226103C1.pdf

cope with costs and power consumption constraints. The distance from the data source generated by the sensors is minimised. The compute resources process this raw data in line and produce insight data with minimal latency. The HW devices of the micro-edge physical sensors/actuators generate from raw data insight data and/or actuate based on physical objects by integrating AI-based elements into these devices and running AI-based techniques for inference and self-training. Intelligent micro-edge allows IoT real-time applications to become ubiquitous and merged into the environment where various IoT devices can sense their environments and react fast and intelligently with a very low power budget energy-efficient gain. AI capabilities integrated into IoT devices significantly enhance their capabilities (functionality, performances, low latency, low power consumption, high processing power) and usefulness, especially when the full power of these networked devices is harnessed – a trend called *AI on edge*[16,17,18].

The ***deep-edge*** comprises intelligent controllers like Programmable Logic Controllers (PLC), Supervisory control and data acquisition (SCADA) elements, machine vision connected embedded systems, networking equipment, gateways and computing units that aggregate data from the sensors/actuators of the IoT devices that generate data. Deep edge processing resources are implemented with performant processors and microcontrollers such as Intel i-series, Atom, ARM M7+, etc., including CPUs, GPUs, Tensor Processing Units (TPU), and ASICs. The system architecture, including the deep edge, depends on the envisioned functionality and deployment options considering that these devices' cores are controllers: PLCs, gateways with cognitive capabilities that can acquire, aggregate, understand, react to data, exchange, and distribute information[19].

The ***meta-edge*** integrates processing units, typically located on-premises, implemented with high-performance embedded computing units, edge machine vision systems, edge servers (e.g., high-performance CPUs, GPUs, FPGAs, etc.) that are designed to handle compute-intensive tasks, such as processing, data analytics, AI-based functions, networking, and data storage[20].

This classification is closely related to the distance between the data source and processing, impacting overall latency. A high-level representation of the edge cloud continuum is represented in **Figure 3** and a rough estimation of the communication latency and the distance from the data sources are presented below.

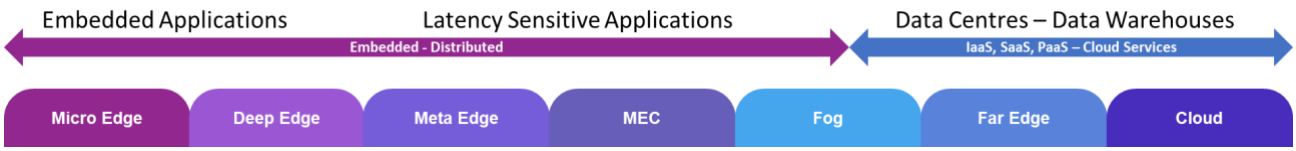


Figure 3 Edge cloud continuum representation

- Micro-edge latency below 1 ms, range from mm to 15 m.
- Deep-edge latency below 2-5 ms, range up to 1 km.

[16] Vermesan, O., Pétrot, F., Coppola, M., Schneider, M. and Höß, A. (Authors). Industrial AI Technologies for Next-Generation Autonomous Operations with Sustainable Performance, in "Intelligent Edge-Embedded Technologies for Digitising Industry" (Chapter 1), River Publishers Series in Communications, June 2022. ISBN: 9788770226110, e-ISBN: 9788770226103. Online at: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788770226103C1.pdf

[17] Dhiraj Joshi; Nirmit Desai; Shyama Prosad Chowdhury; Wei-Han Lee; Luis Bathen; Shiqiang Wang; Dinesh Verma, "AI at the Edge: Challenges, Applications, and Directions," in IoT for Defense and National Security, IEEE, 2023, pp.133-160, doi: 10.1002/9781119892199.ch9.

[18] A. Munir, E. Blasch, J. Kwon, J. Kong and A. Aved, "Artificial Intelligence and Data Fusion at the Edge," in IEEE Aerospace and Electronic Systems Magazine, vol. 36, no. 7, pp. 62-78, 1 July 2021, doi: 10.1109/MAES.2020.3043072.

[19] Vermesan, O., Pétrot, F., Coppola, M., Schneider, M. and Höß, A. (Authors). Industrial AI Technologies for Next-Generation Autonomous Operations with Sustainable Performance, in "Intelligent Edge-Embedded Technologies for Digitising Industry" (Chapter 1), River Publishers Series in Communications, June 2022. ISBN: 9788770226110, e-ISBN: 9788770226103. Online at: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788770226103C1.pdf

[20] Vermesan, O., Pétrot, F., Coppola, M., Schneider, M. and Höß, A. (Authors). Industrial AI Technologies for Next-Generation Autonomous Operations with Sustainable Performance, in "Intelligent Edge-Embedded Technologies for Digitising Industry" (Chapter 1), River Publishers Series in Communications, June 2022. ISBN: 9788770226110, e-ISBN: 9788770226103. Online at: https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788770226103C1.pdf

- Meta-edge latency below 10 ms, range up to 50 km.
- MEC latency 10-5 ms, range up to 75 km.
- Fog latency 10-20 ms, range up to 100 km.
- Far-edge latency 20-50 ms, range up to 200 km.Cloud and data centres latency 50-100 ms, range up to 1000 km.

IoT application deployments at the edge can provide more energy-efficient processing solutions by integrating various computing architectures at the edge (e.g., neuromorphic chips, CPUs, GPUs, ASICs, FPGAs), reducing data traffic and data storage.

Edge computing reduces the latency and bandwidth constraints of the communication network and Internet connectivity by processing locally and distributing computing resources, intelligence, and software stacks among the computing network IoT devices.

3.2 Main Trends, Issues and Challenges

Edge computing moves service provisioning closer to producers and users of such services. It provides low-latency, mobility support, data analytics close to the data source, and reduced energy consumption.

In IoT, there are many expectations for AI-based applications. AI processing happens mainly in the cloud.

With the improvement of AI enabling technologies, AI processing is moving into IoT devices. Intelligent edge devices will integrate software to train the AI model for different applications and executable software that runs the AI algorithms on the IoT devices.

Machine Learning (ML) and Deep Learning (DL) will have unique roles for intelligent IoT devices at the edge.

As a subset of AI, ML enables machines to recognise patterns and make predictions by analysing data instead of using explicit programming. For a higher level of accuracy, ML can be upgraded to DL.

DL is a class of ML algorithms that progressively uses a hierarchy of multiple layers to extract higher-level features from the raw input.

With DL, a computer can train itself with an extensive data set collected for this purpose. The result is an Artificial Neural Network (ANN) that contains all the information to carry out the task. The ANN uses the knowledge acquired in training to infer data features from new incoming data.

Achieving a middleware architecture that integrates all the levels of the edge granularity and manage to effectively handle heterogeneous IoT resources, including networking and computing, is a new challenge for IoT/edge computing, leading to a unified networking and computing architecture.

Deployment of DL at the IoT edge has several challenges such as identification of leading performance indicators of edge DL algorithms, exploitation of trade-offs between the indicators to improve the efficiency of the algorithms, effective combination of the simplified DL models at the IoT edge with the DL model in the cloud, coordination between training and inference and energy-efficient deployment of DL at the IoT edge.

3.3 Research Priorities Timeline

Table 1 IoT and edge computing research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
AI	Develop effective AI-based solutions that can exploit the benefit of DL and Federated Learning In different ways for the different needs of the Edge Granularity	How to deliver an IoT/edge-cloud continuum that takes care of all the specificities of all the Involved layers in a smooth way.	Distinction of the several Edge Granularity totally transparent to both systems and humans (final users).
Accelerators	Adapt, by using dedicated accelerators like ASICs or reconfigurable ones like FPGAs (depending on the constraints and requirements in focus), the different needs of the different edge granularity.	Exploit the smaller technology node so to embed in edge devices advanced accelerators functionalities.	No distinction possible anymore between FPGA and dedicated HW.
New HW architectures	Promising new pre-commercial architectures (like neuromorphic computing ones) will be assessed against existing traditional architectures based on CPU/GPUs or vector processors.	Edge devices containing novel HW architectures that can run AI algorithms so to achieve better results than the currently existing HW architecture based on CPU and GPU.	Synergy between legacy and novel architectures and usage of one or the other according to the real-time needs of the use case in focus, taking into consideration also real-time self-adaptation to the different workloads.
Security	Design a secure-by-construction distributed architecture that can impact all the different granularities of the Edge.	Deploy such architecture across different verticals and industrial domains.	Take on board quantum and post-quantum novel approach to ensure the highest possible security level at all layers and kind of devices in a transparent way for final users.

4. IoT Edge and X-Continuum Paradigm

Distributed IoT digital platforms and infrastructures for collecting, processing, computing, communicating, and running analytics are evolving towards an interconnected ecosystem allowing complex applications to be executed from IoT edge to high-performance computing capabilities.

The IoT digital continuum includes computing resources placed at optimal processing points in the IoT system from the cloud data centre to edge IoT systems and endpoint devices that integrate E2E capabilities such as sensing, processing, connectivity, computing, storage, intelligence, security, safety, and privacy as illustrated in **Figure 4**.

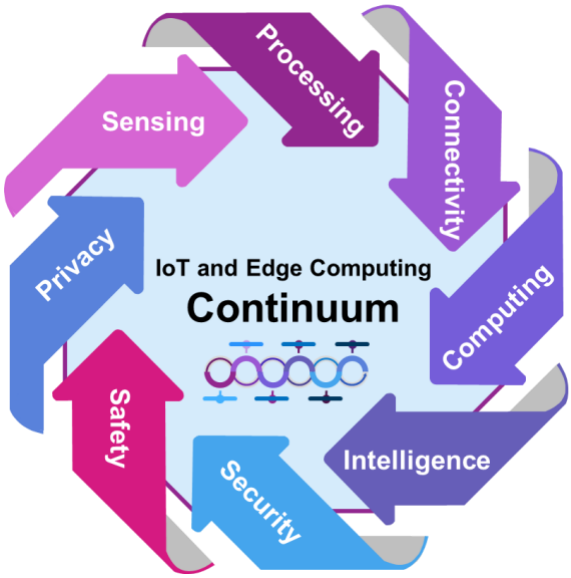


Figure 4 X- continuum paradigm

Implementing IoT E2E capabilities in such a distributed continuum is challenging and requires reconciling different application requirements and constraints with IoT infrastructure design choices including the energy consumption continuum.

One main challenge in this domain is how to accurately reproduce relevant behaviours of IoT applications workflow and representative settings of the IoT physical infrastructure, including AI-based learning/training and inferencing underlying the complex distributed continuum from micro-, deep-, meta-edge to cloud.

4.1 Technological developments

IoT data processing, computing and communication no longer lean only on traditional approaches that send all data to centralised cloud facilities for processing, rather leverage on the distributed resources close to where the data is generated, so to extract insights in real-time while keeping efficient resource usage and preserving security and privacy constraints.

The IoT digital continuum seamlessly combines resources, processing, and storage capabilities, and services at the centralised cloud, IoT edge, and in-transit, along the distributed data path.

The development of different dedicated systems for data processing on each component of the continuum lacks a holistic approach and a trustworthy architecture for implementing future IoT ubiquitous computing systems. One of the main challenges in this context is related to the complexity of deploying large-scale, real-life IoT applications on such heterogeneous infrastructures, which breaks down to configuring many system-specific parameters and harmonising many requirements or constraints regarding processing, communication latency, storage, energy, network efficiency, interoperability, mobility, security, and data privacy.

The IoT digital continuum requires an IoT digital infrastructure jointly used by complex application workflows, commonly combining real-time data generation, processing, computation, and analytics.

The combined edge-cloud infrastructures deliver IoT applications' virtual distributed-centralised computing and storage resources to perform stream and batch analytics on comprehensive historical data, AI model training, and complex simulations. IoT edge infrastructures complement these virtual resources with distributed computing and storage capabilities close to IoT intelligent devices that sense the environment.

The IoT elements include nodes, programable logic controllers, gateways, routers, micro-servers, and embedded high-performance units distributed across the edge continuum and used for final or in-transit processing on data aggregated from multiple IoT edge devices to reduce further data volumes that need to be transferred and processed in the clouds and data centres.

Lightweight frameworks, based on message brokers using IoT lightweight protocols, enable distributed and hierarchical processing and intelligent aggregation, minimising latency, and bandwidth usage.

The IoT digital continuum requires an efficient architecture that focuses on both horizontal and vertical resource distribution in the IoT edge-to-cloud continuum to secure seamless E2E services across the whole continuum. As a result, IoT system architectures and management mechanisms are needed to seamlessly encompass computing, storage, and networking.

4.2 Main Trends, Issues and Challenges

The implementation of IoT continuum-X requires research that integrates ideally open-source intelligence tools, HW and SW platforms, and systems, thus addressing the non-functional aspects of IoT systems with multiple elements as part of the continuum-X.

Another issue is how to guarantee embedded interoperability into continuum-X with transparent aggregation, distribution and logging of participants and system activities when using IoT distributed edge computing services.

The research effort must address how to collect simultaneously a huge amount of data from a very disperse, heterogeneous and numerous numbers of sources when real-time decisions are to be taken.

Future research activities include addressing the resource management for continuum-X capabilities by managing the resources on the processing points and identifying the optimal E2E capabilities and their relevance, depending on the IoT application context.

Work is required on providing solutions for dynamic placement of edge computing platforms to minimise the network access delay depending on the context, IoT activity at the edge and IoT application scalability requirements.

Further research is needed to provide collaborative and hierarchical computing to distribute the IoT devices' workload among various distributed processing/computing points and allocate optimal resources to each device based on the continuum-X capabilities and requirements.

The research in the following years should address the infrastructure edge and the device edge together and provide solutions for optimising the integration of the two.

Research in context-aware, scalable heterogeneous continuum-X optimisation for IoT applications is required due to the tremendous diversity of workloads and applications being run across a variety of different IoT edge devices.

Security, safety, and monitoring of critical E2E capabilities of IoT systems are essential for many IoT applications. The integration of solutions for addressing these elements of the continuum-X holistically into IoT platforms should be prioritised.

To provide continuum-X implementation flexibility on different IoT platforms, new research directions should address developing and deploying containers at the edge that address challenges related to connectivity, distribution, and synchronisation, and leverage the different IoT architecture to deploy new solutions and applications. Developing edge AI for IoT applications requires offloading AI models learning/training to IoT devices to retrain the AI models locally with near real-time data collected by the IoT devices for efficient data processing.

Future research is required to identify how the computational tasks, AI models, inputs, parameters, and weights, are instantiated on IoT devices considering the specific requirements for the continuum-X elements and how their allocation changes during execution.

Addressing IoT distributed AI and federated learning/training considering the continuum-X elements requires defining a new generation of tools and mechanisms that enable fine-granularity computation, processing, communication, coordination, and mobility management across the edge.

Finally, new research approaches are required to address the fragmentation in IoT to tackle the E2E challenges, by providing several interoperable, integrated HW, software, and services approaches to address the continuum-X.

4.3 Research Priorities Timeline

Table 2 IoT edge and X-Continuum research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Continuum refinement	High-level IoT-edge-Cloud continuum solutions for basic services, protocols, and resource allocation.	More refined continuum support of functionalities and lower layers management.	Fully supported and smooth management of all the edge granularities, types, services resources, and functions, in a fully heterogeneous ecosystem.
Common shared data space	Definition of domain-specific edge IoT applications aligned to common European data spaces.	Definition and implementation of common European data spaces.	Fully compatible interwork of data spaces with all geographical areas.
Instantiation	Piecewise and vertical-specific instantiation of all kinds of resources.	Coherent and homogeneous instantiation of all kinds of resources.	No distinction between the kinds of resources, all are treated as If they were homogeneous and available everywhere.

5. Intelligent Connectivity

Networks and connectivity are becoming more heterogeneous and IoT devices use more and more a variety of equipment with different wireless access technologies. With the constant increase of the numbers of users (new contracts) and especially of things (sensors, metering systems, mobile/static robots, vehicles, drones, etc.) joining each day the communication network, the need for a smarter and more effective way of handling the related growing data created by those devices is becoming more and more an issue that needs the attention of the IoT community.

To handle such complexity and to manage in a smart way how the communication system can properly manage such an increasing amount of data (scalability problem), there's the need to define and elaborate on the intelligent connectivity concept, to optimise the usage of the networks but also to decrease the overall energy consumption of the overall IoT system.

Intelligent connectivity can be seen as the smooth synergy of different technologies and domains, so to offer final users of a communication system the best possible QoS, according to the given resource, available technology, and energy constraints.

5.1 Technological developments

With the technology miniaturization that still proceeds at almost yearly cadence, and recent advancements in battery technology, and the more effective use of out-of-device processing capability services and applications, it is possible to increase the number of functions and the communication capabilities of terminals, so to properly handle most of the issues described above and make intelligent connectivity finally a reality.

The next wave of IoT devices at the edge will therefore use a kind of intelligent connectivity that relies on the consolidation and synergy of different communication technologies. Whereas the Internet is today the largest worldwide communication network, such intelligent connectivity for IoT still requires further development to allow high demand in bandwidth and quality in signals and protocols, in support of more critical content and data exchange.

The requirements of real-time response may be, amongst others, safety and mission-critical (like in telemedicine, for example) and, consequently, IoT communications solutions are numerous and diverse:

- ***Artificial Intelligence***, especially when declined in distributed AI at the edge of the network, but also as a set of methods to more intelligently manage the huge and diverse amount of data created and consumed by terminals.

- ***Advanced communication protocols***: to accommodate the different needs of the different verticals that make use of the communication network, dedicated and always improving communication protocols are to be defined and deployed. Standards bodies constantly update and add new features to each new generation of the network they define.

- ***Edge Processing***: the need for low latency of several applications and the complexity of the data to be managed request that always more data shall be handled and processed as close as possible to the source and destination of that data, i.e., at the edge. The Multi-Access Edge Computing (MEC) concept, in constant evolution, and its related features can be seen as a cornerstone in the quest for a more efficient data management at the Edge.

- ***Energy Consumption***: this is a system parameter that becomes more and more important at each new generation of the communication network. Reason for that is not only the need for CO2 reduction to tame the disruptive climate change consequences, but also sheer economic reasons, as increasing the number of servers and chips needed to handle the raising amount of data exchanged in the world, implies a constant and steep raise of the energy demand to accommodate the needed QoS and reliability of such communications. Therefore, it is key that in the forthcoming Intelligent Connectivity paradigm low energy consumption is taken as a key design constraint for all new chips, platforms, and SW suites.

- ***Spectrum management***: with the introduction of several access technologies (LoRa, Wi-Fi, cellular, etc.) and the commercial availability of new spectrum bands for new application (mmWave bands under and above 100 GHz in addition to the standards sub-6 GHz bands), there is the need to make effective use of all the different bands now made available. That effective use has the advantage not only to increase the coverage, the resiliency, and the performance, but also, to enable offering the lowest energy consuming access technology in a specific vertical use case, also reducing in a dynamic way the energy consumed to deliver a specific service. Dynamic usage of different kind of spectrum, of non-adjacent bands, and even mixing different bands coming from different access technologies, based on local availability, will change the way services can be delivered from the cost and from the quality points of view. Finally, it is worth mentioning that also drones and satellite accesses and related bands will soon be broadly available for commercial use, and the availability of coverage everywhere will change the way we think of connectivity and related services.

- ***Multi-Access capable devices***: to deliver higher QoS, to handle the communication bottlenecks (both in the front- and the back-haul) in highly densely populated areas, and to fulfil Key Performance Indicators (KPI) of the applications requesting a huge amount of bandwidth, e.g., for Augmented Reality / Virtual Reality (AR/VR) services, the need of a handset capable of making use of the most suitable available access technologies and bands is becoming more and more important.

- ***Seamless connectivity broker:*** that is needed to optimise the connectivity to a specific network, according to several technical and business parameters. The seamless roaming should avoid that data get lost during the switching procedure; AI/ML technologies should also contribute to make the most relevant choice.

An essential characteristic of the next generation IoT is the requirements range from high reliability and resilience in the communication network to ultra-low latency and increased capacity at the communication channel. IoT Intelligent Connectivity solutions are also very dependent on the context in which they are applied and whether it is necessary to respond to strict energy efficiency constraints or cover large outdoor areas, deep indoor environments or vehicles moving at high speeds.

5.2 Main Trends, Issues and Challenges

The next-generation IoT must address the convergence between different cells and radiation and develop new management models to control roaming while exploiting the coexistence of many different cells and radio access technology (RAT). New management protocols to handle user assignments regarding cells and technology will have to be deployed in the mobile core network to access network resources more efficiently.

Satellite communications is becoming a commercial reality and is to be considered as a new RAT, especially in remote (white spot/blind spot/not spot) areas. With the emergence of safety applications, minimising latency and various protocol translations bring tangible benefits to E2E latency.

AI/ML will bring significant disruption to future networks from impacting the design of air interface, data processing, network architecture and management towards computing for achieving superior performance. It will become essential for E2E network automation dealing with the complexity of orchestration across multiple network domains and protocol layers.

Network intelligence will help to improve energy efficiency and ensure service availability by performing optimisations challenging for traditional algorithms with AI/ML approaches and carrying out system management tasks autonomously with AI/Machine Reasoning (MR).

An autonomous system can only be successful if trusted by humans and can be understood and explained. It is highly critical to establish suitable mechanisms for explainable AI and trustworthy AI.

For example, the system needs to be able to explain its actions and why it ended up in its current state; the intelligent system should i) act lawfully, respecting all applicable laws and regulations, ii) be ethical, respecting the right principles and values, and iii) be technically robust while considering its impact on the social environment.

At the edge of network coverage, a temporary network coverage extension might be required to provide connectivity between several autonomous vehicles during operation. The connectivity should remain even when the vehicle platoon leaves the network coverage entirely while still in operation.

Industrial vehicle manufacturers can have fleets of shop-floor vehicles deployed in a factory. While all or some of them are connected to the wide-area network, the application may require having reliable networking solutions between the vehicles not using the local network, i.e., using a non-public-network (NPN), a local private infrastructure-less network being established.

This network might have authorised access to the spectrum of a local NPN or a public network; thus, external network control should be enabled. an important part of this scenario is also Device-to-Device (D2D) communication, a feature which exists in 5G, and will be further enhanced in the forthcoming generation of standards.

Mesh networks, multi-D2D might be different options for implementation. In many scenarios, temporary, ad-hoc security solution deployments are required. Networking islands of several devices re-joining the cellular networks shall be seamlessly re-integrated. D2D could be seen as a first step, and Data Management Object (DMO) solutions are known from several standards.

The mesh wireless networks provide simpler topology using direct communication between edge IoT devices, increase stability as single points of failure don't damage the whole network and increase the range. The mesh topology ensures better security with lower power consumption for each edge IoT node.

The challenges that need to be addressed in developing the next-generation wireless mesh technologies are related to cost, scalability, latency, and complexity.

In this context more research effort must be spent in finding new solutions for providing interoperability between edge IoT devices and platforms in the direction created by Matter[21] and Thread[22].

Matter allows the edge IoT devices to work offline without requiring continuous access to the cloud and different cloud services. Matter strengthens the wireless connectivity landscape covered by protocols such as Zigbee, Z-Wave, Bluetooth, and Wi-Fi. This is an important development considering the evolution of Wi-Fi 6, Wi-Fi 6E and Wi-Fi 7and the use of 2.4/5/6 GHz bands.

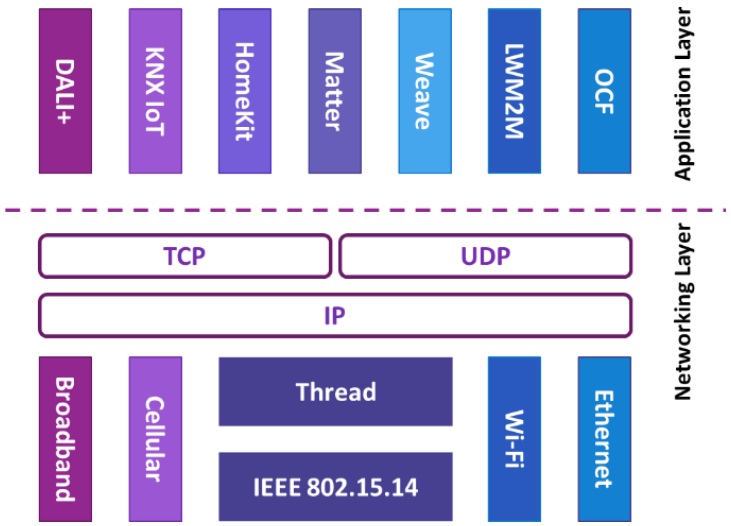


Figure 5 Matter and Thread edge IoT connectivity.

Wi-Fi is based on the IEEE 802.11ax or 802.11ax-2021 specification and branded as Wi-Fi 6 by the Wi-Fi Alliance and can operate in license-exempt bands at 2.4 GHz, 5 GHz, and 6 GHz.

Further improvements gave room to a newer release, called Wi-Fi 6E[23] (where E stand for Extended), the main innovation of which is to leverage the 6 GHz band for unlicensed operation, the availability of which strongly depends on country-specific regulations.

Wi-Fi 7, Wi-Fi Extreme High Throughput, based on the IEEE 802.11be standard is bringing further improvements such as increased throughput: from 9.6 Gbps of Wi-Fi 6 to 46 Gbps, support of 320 MHz channels, Multi-Resource Unit (RU) (also known as puncturing), allowing to exploit non-contiguous spectrum bands and deterministic low latency.

[21] https://csa-iot.org/

[22] https://www.threadgroup.org/

[23] https://www.wi-fi.org/

Wi-Fi 7 continue the work to enhance support for IEEE TSN (Time-Sensitive Networking) capabilities. Existing Time Sensitive Networks (TSN) features, such as time synchronisation and scheduling, will be improved in the future with a higher degree of determinism and higher reliability.

Thread is a low-powered mesh-based wireless protocol that complements Matter by creating a low-latency offline environment that instantly sends and receives data across devices. The Thread wireless protocol into the mix can also achieve complete offline computing within your local mesh network of IoT devices.

A future connectivity challenge for edge IoT is to facilitate seamless roaming between available connectivity (5G, Wi-Fi, LoRa, etc.). A device should be able to connect to the most suitable network given the connectivity requirements (latency, bandwidth, security, energy consumption, etc.) but also the cost, the location, and the end user preferences.

The concept should be optimised and aligned with the approach proposed by 3GPP called access network discovery and selection function (ANDSF) that should be extended to IoT Networks. Such connectivity broker / ANDSF should take advantage of AI/ML technologies to optimise the choice and avoiding extensive roaming.

5.3 Research Priorities Timeline

Table 3 Intelligent connectivity research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Mesh connectivity	Extend the mesh connectivity to different protocols e.g., LoRA 2.4GHz and dual-band transceivers, low-power and higher data rates.	Wi-Fi development and enhance support for TSN for industrial environments. AI-based cognitive solutions for mesh network management and mesh topology scalability.	Mult-protocol, multi frequency modules for autonomous edge IoT devices and vehicles. Seamless wireless/cellular connectivity for autonomous distributed systems. Ultra-low power, higher data rate mesh heterogenous mesh network architectures.
Interoperability	Seamless roaming between available wireless (including cellular) connectivity. Interoperability solutions for edge IoT connectivity in heterogenous applications and across industrial sectors.	E2E network automation and orchestration across multiple network domains and protocol layers. Interoperability solution for self-configuration, self-healing	Interoperability solution for high precision location and positioning services across heterogenous wireless networks.
Satellite	Advance the development on nanosatellites for IoT applications and the integration with terrestrial edge IoT infrastructure.	Research on management protocols deployed in the mobile core network to increase the efficiency of accessing network resources and reduce the energy consumption.	Satellite-cellular-wireless continuum for edge IoT applications.

6. Energy-Efficient Intelligent IoT and Edge Computing Systems

The number of IoT applications is constantly increasing, due to the fact that more and more IoT devices are being deployed in different industrial sectors.

Such IoT applications are consuming increasing amounts of energy, and new technologies and methods need to be developed to increase the energy-efficiency of the IoT devices, AI algorithms, architectures and IoT systems to reduce the overall power consumption.

Next-generation IoT edge applications and networks need greater flexibility to implement edge utilisation mechanisms to maximise energy-efficiency, latency, processing, data transfer, and dependability.

From the IoT system architecture perspective, the technological trend is to move the data processing and analysis from cloud to edge. This shift requires that the edge IoT devices in the edge micro-, deep- and meta-edge domains (e.g., sensors/actuators, microcontrollers, end-devices, gateways, edge servers) become more energy-efficient and support AI techniques at low power consumption to ensure high autonomy/longer battery life, system availability and reliability.

To make such shift happen, a new generation of more performant processing units and new architectures (e.g., neuromorphic and hybrid) are needed, which can guarantee the best trade-off between communication power and ultra-low power consumption and increased intelligent processing needs.

6.1 Technological developments

The move of the data processing to the edge and the implementation of distributed IoT computing architectures require optimising the location of processing and the transfer of intelligence where the application needs it (e.g., micro-, deep, meta-edge).

Energy-efficient and green IoT requires a holistic E2E strategy through the IoT architectural layers across the information value chain to address the entire edge IoT systems energy-efficiency continuum and energy management. This energy-efficient design optimisation is required for green IoT components and algorithms at each IoT architectural layer level.

Combining energy-efficient AI and IoT technologies at the edge can maximise the IoT capabilities across the architectural layers and optimise the whole IoT system, including the application domain.

Edge IoT and AI green designs (e.g. advanced and adequate semiconductor technologies, efficient design, energy-efficient SW/HW platforms) are needed for providing environmentally reliable components at all IoT architectural layers and functions, energy-efficient and low CO_2 footprint at IoT infrastructure and technical solutions (edge, hybrid edge-cloud, AI-based learning/training, etc.), and finally also allowing the deployment of green manufacturing (e.g. manufacture IoT electronic components, HW/SW platforms, and IoT systems with minimal or no impact on the environment).

The implementation of green IoT and AI energy-efficient techniques and methods (optimisation, trade-off analyses among crosscutting functions/system properties vs. energy, green IoT/AI metrics, performance, measurement, testbeds, energy harvesting, wireless power transfer, etc.) depends on the functions performed by different HW/SW/algorithms components integrated into the IoT architectural layers.

These techniques include energy management, wake-up scheduling mechanism and selective sensing, HW/SW partitioning, energy-efficient methods/algorithms, communication techniques and distribution of task, efficient IoT nodes and resources on multi-core, minimisation of data path length, data buffer delivery, wireless communication, processing of trade-off communication.

6.2 Main Trends, Issues and Challenges

More edge IoT devices and applications are deployed together with intelligent edge IoT platform solutions used to collect, process, analyse the IoT device-collected data while making decisions and taking actions. AI is applied to most of these edge IoT devices to implement the future Internet of Intelligent Things.

Wireless and cellular communication technologies enable for collection of even more significant amounts of data from intelligent edge IoT devices.

The increase in the connected edge IoT devices, combined with the distributed computing model introduced by edge computing, reduce latency and the amount of data that needs to be sent between the central cloud and the edge IoT devices, saving bandwidth costs.

The IoT edge model extends security benefits, and the localised edge processing allows autonomous control of devices when the communication networks are jammed, or the connection is lost.

The capabilities, performance, responsiveness, and energy-efficiency of the IoT edge processing models are increased due to reduced data transmission and distributed processing.

The next-generation IoT and AI edge solutions should focus on novel energy management techniques to select energy sources, energy harvesting techniques, HW/SW/algorithms optimisation for data sensing, monitoring, filtering, prediction, and compression.

Processing combined with sleep/wake-up techniques, energy-efficient task scheduling algorithms, selection of Quality of Information (QoI), allocation of workload distribution at the edge are used together with wireless communication optimisation (send/receive), power down mechanisms to improve the energy-efficiency of IoT systems.

The dynamic wireless network behaviour (e.g., IoT devices-move-in and IoT devices-move-out) is monitored, and the cooperation/information exchange between the edge IoT devices (with optimised green and energy profiles) is optimised to increase the overall IoT system energy-efficiency.

The integration of ML and AI methods support the optimisation of IoT/edge computing-based green and energy-efficient functions providing solutions for moving the processing optimally from cloud to the edge and decarbonising the whole value chain of IoT information.

The optimisation for energy-efficiency and green IoT requires the use of federation and orchestrations techniques that create dynamic and distributed energy control frameworks for edge IoT applications.

The implementation of energy efficient IoT intelligent search engines, cooling systems, and energy harvesting techniques and renewables must be considered when the HW/SW/algorithms components of the IoT application layer are evaluated.

New IoT applications, including AR/VR, DTs, virtual simulations, real-time searching engines and discovery services, bring new challenges to optimising energy-efficiency as the virtual simulation and the AI, learning/training algorithms, are increasing the energy consumption of the whole IoT system that will have two components one physical and one digital/virtual.

The complexity of intelligent IoT applications at the edge requires designing, analysing and optimising the energy-efficiency at the IoT system level by considering the aggregation, over the technology stack, of the functions required to fulfil a given IoT task. This includes estimating the energy used for learning/training of different algorithms implemented in various IoT architectural layers, both during inference and learning by employing real data sets from different databases, the energy consumption of the edge IoT devices (micro-, deep-, meta-edge), the energy consumption of the communication networks and the other processing and storage units by the IoT application, for performing different tasks and services.

Currently, most of the embedded IoT devices and as well low-power IoT sensors are powered by batteries which need to be replaced every few years due to their limited lifespans. Usually, the replacement of these batteries can be costly and therefore solutions on enabling energy efficiency for communicating IoT devices and embedded systems can be very beneficial for the energy footprint of future IoT systems.

One of the most promising approaches to remove the dependency of batteries is the harvesting of energy from naturally or artificially available environmental resources.

Another approach is to increase the energy efficiency by decreasing the battery power needed by IoT devices and embedded systems.

Further needed research activities include improved energy management approached to reduce the energy footprint of IoT devices and embedded IoT devices by enabling the use of both mentioned approaches: energy harvesting and increasing energy efficiency.

6.3 Research Priorities Timeline

Table 4 Energy-efficient intelligent IoT and edge computing systems research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Energy harvesting	Research on hybrid solutions combining ultra-low power connectivity with energy harvested from ambient radio frequencies (RF), thermal, kinetic, and photovoltaic (e.g., solar, and indoor/outdoor lighting) energy sources.	Multi energy harvesting, wireless power for edge IoT devices. Energy harvesting solutions at mesh network edge IoT devices.	Energy harvesting for edge IoT devices integrating positioning and sensing. Cognitive energy management orchestration in edge IoT systems for data processing energy optimisation.
Energy-efficient hardware	Research on the next-generation of energy harvesting ultra-low-power devices with on-demand wake-up feature integrated into edge IoT applications	Edge IoT devices base on printed electronics (e.g., conductive inks, metal etching, laser-direct structuring (LDS) for printable circuits and batteries) to be embedded in objects and products. Energy harvesting for edge IoT devices integrating machine-vision camera systems using AI and ML.	Research on energy-harvesting interfaces for kinetic energy harvesting from heterogenous generators (piezoelectric, triboelectric etc.).
Energy-efficient data processing	System-level optimisation techniques combining lower power consumption and energy harvesting technologies. E2E energy methods and models for data compression and exchange in edge-cloud IoT platforms.	Benchmarking methods for energy-efficient and low CO_2 footprint of edge IoT infrastructure and technical solutions.	Energy-efficient data aggregation mechanisms in intelligent edge IoT systems considering the associated processing capabilities across the computing continuum.

7. Heterogeneous Cognitive Edge IoT Mesh

IoT edge can be formed by a mesh network of intelligent IoT devices using edge IoT platforms, including AI model training and ML inference that process, analyse, store information locally close to the data sources, and communicate and exchange information with other edge devices, computing units and across the computing continuum, made of cloud platforms and data centres.

Cognitive compute continuum applied in decentralised environments, including edge mesh infrastructures, can operate efficiently and reliably without a central entity for full knowledge and management about available resources and current workloads.

Autonomous computing techniques and ML should be broadly applied, so to be able to adapt to unforeseen situations and anticipate future circumstances, such that the cognitive edge IoT devices become self-aware, self-managed, self-protected, self-healing, and self-optimising.

7.1 Technological developments

IoT and edge computing systems evolve around the fundamental context management processes: acquisition, modelling, reasoning, and distribution, while distributing the processes based on the context information.

Novel IoT and edge computing designs bring innovative adaptive and behavioural-awareness capabilities to the IoT, so to set the foundations for developing the next-generation cognitive and self-adaptive IoT systems.

The huge number of heterogeneous edge IoT devices need to be integrated into mesh networks, in which the infrastructure nodes connect directly, dynamically, and non-hierarchically to other nodes and cooperate with one another to efficiently route data to and from edge IoT devices.

The mesh network topologies allow multiple routes for exchanging information among connected nodes. The mesh approach increases the network's resilience in case of a node or connection failure.

More extensive edge IoT mesh networks may include multiple routers, switches and other IoT devices operating as nodes. In heterogenous cognitive IoT networks, context-awareness is becoming critical for IoT systems as the processing is moving towards pervasive, swarm evolutionary computing.

Resources and services are remotely accessed by edge IoT devices from anywhere in the network at any time. The environment in which data is exchanged and processed can change dynamically as different ad-hoc heterogenous networks are created.

Creating self-configured mesh IoT networks, where things integrate self-perception and automated response, can support this.

Embedding appropriate plug-and-play intelligent and autonomous edge IoT devices facilitate the transition into IoT networks with self-X capabilities (self-configuring, self-healing, self-optimising, self-protecting, etc.).

Such self-configured mesh IoT networks form a flexible architecture where things are active and locally integrate almost every functional and operational requirement.

The IoT end-devices can manage critical aspects such as security, safety, and trustworthiness and embed federated, decentralised ML and decision-making mechanisms, enabling disruptive cross-domain applications with high complexity and scale.

The security techniques used by edge IoT devices can be crucial for obtaining contextual information from other end devices using a lightweight and E2E approach based on current standards (e.g., IETF OSCORE24). The process is linked to an initial bootstrapping by which a legitimate device can be successfully and securely deployed in the network.

The modelling of context information should be based on current standards that guarantee the representation format's interoperability using flexible approaches (e.g., JSON-LD25, or additional representations based on CBOR26). In this case, the primary purpose is to achieve a trade-off between lightness and expressiveness to represent the dependencies among devices' contextual information.

7.2 Main Trends, Issues and Challenges

The evolution of IoT and edge computing system will be based on the integration of AI-based mechanisms. Moving part of the system intelligence down to the end devices brings a range of advantages and allows a widespread collective-intelligence web.

The use of intelligence on the device (e.g., TinyML27 and other similar embedded ML applications, algorithms, HW, and SW) boosts the evolution of end devices to intelligent IoT objects that can offer, among other advantages, a much more autonomous behaviour.

Integrating AI within edge IoT devices is one step towards developing cognitive and evolutive IoT systems. The integration of cognitive self-evolution capabilities in the entire E2E network chain (edge, dew, fog, and cloud) goes beyond the current limits of AI by permitting end devices and, by extension, the whole system to grow and refine its intelligence.

The development of evolutive artificial cognitive mechanisms and their integration with the self-x concepts pave the way for designing IoT devices and systems with increased intelligence that will permit them to meta-learn from new situations, scenarios, and environmental changes.

The cooperation among individual meta-smart IoT objects can create a higher intelligence layer for tackling large-scale issues. The decision process is not isolated but starts from a complete view of the scenario and gathers collaborative efforts.

The heterogeneous cognitive and mobile IoT edge mesh solutions utilise low-level IoT devices for the decision-making process, the gateway devices and the micro servers distributed across the edge continuum. The data collection, processing, and decision-making tasks are distributed among these edge devices within heterogeneous networks.

The computation tasks and data are shared using a cognitive mesh network of edge IoT devices, gateways, and micro servers. Heterogeneous cognitive and mobile IoT edge mesh systems offer distributed processing, low latency, fault tolerance, better scalability, security, and privacy. These features are essential for critical applications that need higher reliability, real-time processing, mobility support, and context awareness.

[24] https://datatracker.ietf.org/doc/rfc8613/

[25] https://json-ld.org/

[26] https://cbor.io/

[27] https://www.tinyml.org/

Distributed computations on edge IoT systems imply addressing heterogeneous cognitive features for IoT applications and developing a fault-tolerant robust collective computing framework suited for multi-IoT device systems that include decentralised operations applied to dynamic environments.

Mobile IoT edge mesh characteristics, such as scalability, heterogeneity, mobility, and ubiquitous networking, require a robust cooperative and cognitive computing framework that addresses the edge IoT systems characteristics, including new security solutions adequate to these new IoT-based systems.

The research needs to provide IoT platform-agnostic solutions with scalable edge IoT devices in a self-healing and self-organising network. In a heterogeneous mesh network environment, communication and cognitive coexistence are critical to allow maximum robustness to RF disturbances and minimize negative effects due to the co-existence of various wireless and cellular networks.

The cooperation between edge IoT devices and the dynamic communication infrastructures of the edge and swarm systems create the heterogeneous cognitive and distributed intelligence framework needed to optimally support edge IoT mesh applications.

The heterogeneous cognitive and mobile IoT edge mesh research must address topics at the intersection between IoT, AI, connectivity, and edge computing. These topics relate to context awareness, autonomous control, ambient intelligence, semantic reasoning, and cognitive IoT to enable distributed intelligence in IoT.

The edge IoT distributed intelligence must be addressed holistically by developing cognitive platforms integrating features such as distributed data collection, data analytics, networking, data management, edge IoT device management, resource management, service management, orchestration, and federated learning.

Several research questions are related to defining the distributed mesh network and the cognitive computing model, the distribution of data processing, and the global optimisation (energy, processing, time, etc.) of communication and computation. New computation algorithms must be developed for distributed computing to be performed by the various heterogeneous, resource-constraint edge IoT devices operating with dynamic communication and intermittent connectivity.

7.3 Research Priorities Timeline

Table 5 Heterogeneous cognitive edge IoT mesh research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Architecture	Architectural models and meta-embedded operating systems with integrated stack for wireless mesh networking.	AI-based cognitive mesh architectures that integrate components and modules addressing context awareness, autonomous control, ambient intelligence, semantic reasoning, and federated learning.	Dynamic cognitive mesh architectures with AI and context-based configuration capabilities integrating features for swarm intelligence and distributed processing capabilities.
Cognitive Capabilities	Evolutive artificial cognitive mechanisms for edge IoT systems and the integration with mesh networks topologies.	Development of new algorithms and SW/HW self-X capabilities.	Integration of cognitive self-evolution capabilities in the entire mesh network and across the edge granularity including scalable AI capabilities across the continuum.
Computing Models	Computation algorithms for distributed computing applied to different heterogeneous, resource-constraint edge IoT devices across the edge continuum.	Heterogeneous cognitive edge IoT mesh frameworks integrating features such as distributed data collection, data analytics, networking, data management, edge IoT device management, resource management, service management, orchestration, and federated learning.	Meta-mesh computing models for global optimisation (energy, processing, time, etc.) of distributed systems.

8. IoT Digital Twins, Modelling and Simulation Environments

An IoT DT is a virtual representation of an IoT device that models the device's characteristics, properties, environmental conditions, behaviours, and functions over the operational lifetime, based on real-time data and information synchronised automatically and bi-directionally at a specified frequency and accuracy. An IoT DT uses simulation, ML, and reasoning to simulate various scenarios in different IoT applications and help optimise and improve the overall IoT system functionalities and services.

The real-time feature represents a vital characteristic to define IoT DTs, considering that the real-time instances vary according to IoT applications. In many IoT applications, time values are not defined identically, and such issue should be carefully considered when designing IoT DT instances. The synchronisation between the physical IoT device and its virtual representation in the simulation environment and the synchronisation of the events and scenarios in the simulation platform is critical for the performance of the whole IoT system.

8.1 Technological developments

IoT DTs support optimal decision-making and effective and efficient actions of the IoT devices in IoT applications, using real-time and historical data to represent the past and present and simulate predicted activities tailored to use cases based on domain knowledge, and implemented in Information Technology / Operation Technology (IT/OT) systems. The IoT DTs can expose a set of services to execute certain operations and produce data describing the physical activity of the IoT devices that they virtualise.

How to choose and optimize characteristics, properties, environmental conditions, behaviours, and functions over the operational lifetime of an IoT device that are mapped to the IoT DT is a matter that needs further research; moreover, further analysis is needed also to properly develop IoT DT user interfaces that can connect the IoT DTs with other devices, with humans, and with other DTs coming from different domains (e.g., telco DTs or connectivity DTs).

The lifecycle evolution of the IoT DTs must take into consideration the updatability and upgradability of the IoT devices, including new features addressing the dependability characteristics.

Operational intelligence is used to build IoT DTs as it supports digitising the IoT and edge computing infrastructure, monitoring operations in real-time, predicting events, taking actions based on intelligence and engaging with different stakeholders.

The virtual representation of an IoT DT reflects all the relevant dynamics, characteristics, critical components, and essential properties of the IoT physical device throughout its life cycle. The creation and update of IoT DTs rely on timely and reliable multi-sense wireless sensing, while the cyber-physical interaction relies on timely and dependable wireless control over many interaction points, where wireless interfaces of the IoT device are embedded.

In future networks, IoT DTs will be a valuable tool to create novel and disruptive solutions, especially for vertical industries, that are enabled by a large scale of real-time, robust, and seamless interactions among, for example, machines, humans, and environments.

IoT DTs need to be scaled up in IoT applications, thus enabling for the broadest possible population a sustainable living with systematic climate mitigation measures, improving society's resilience in crises by actively monitoring and simulating a huge number of future scenarios, and potentially helping transform the whole societal structure, so to make it more robust and capable of addressing the environmental (but not only) challenges of the future.

IoT DTs must possess a minimum set of attributes to be integrated into IoT applications and platforms to optimise the functions and services of these applications. These IoT DT attributes are summarised below:

- Abstractness – free from details which are specific to implementations.
- Correctness – give a correct replication of the IoT ecosystem and its devices.
- Completeness – updated vis a vis the functionality in the real-world system.
- Expandability – adapt easily to emerging technologies and applications.
- Parameterised – accessible for analysis, design, and implementation.
- Reproducible – be able to replicate the same result for the same input as the real system.
- Scalability – must be able to operate at any scale.
- Soundness – exhibit only the functionality available in the real-world system.

IoT DTs will continue to grow in industrial and production environments, leading to the new designing approach called massive twinning. It will enable to go beyond the current levels of agility of production, thus allowing more efficient interaction of production means to encompass a more significant extent of the respective processes, and achieve the transfer of massive volumes of data, as well as, often, reach unprecedented performance and reliability levels. The evolution of edge IoT digital twin technology is illustrated in **Figure 6**.

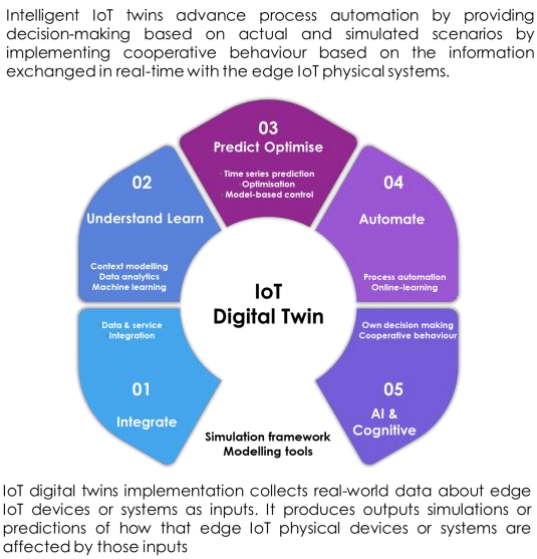


Figure 6 Edge IoT digital twin technology evolution

IoT DTs, as part of IoT technologies and applications, are being expanded to support more applications, use cases and vertical industries, as well as combined with more technologies, such as speech, augmented reality for an immersive experience and AI capabilities, enabling to look inside the IoT DT by eliminating the need to go and check the physical IoT device.

8.2 Main Trends, Issues and Challenges

The research today focuses on developing the virtual model representation of an IoT device, the evolving data sets relating to the IoT domain, the mechanisms to dynamically synchronise and adjust the virtual representation following the changes into the physical IoT device, and the simulation environment in which the IoT DTs will operate.

The IoT DT mapping of the physical environments into the digital world is facilitated by IoT simulation platforms and SW leveraged to create a digital model and a virtual representation of the physical IoT device. IoT digital virtual representation can be used to manipulate and control the real-world IoT device through a teleoperation DT modelling solution.

The research areas for IoT DTs must consider the scope and augmentations of the IoT DT and the operational environment combined with the functions needed to realise the IoT DTs' communication capabilities, and the update frequency required for providing the optimal precision of the IoT DT, based on data measured and acquired during the operation and use of physical IoT devices.

Further research needs to investigate the different levels of IoT and edge computing intelligence through cognitive functions, implemented in the physical/digital and virtual devices.

Understanding, defining, and designing the simulation capabilities of the future IoT platforms, which will be able to provide different fidelity levels of simulation tuned by input parameters, time dependency, behaviour, and prediction aspects, intelligence, and IoT device complexity, are very challenging tasks, which require further investigation.

8.3 Research Priorities Timeline

Table 6 IoT Digital Twins, Modelling and Simulation Environments research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
IoT DT Models	Aggregation of heterogeneous IoT DT models.	Energy-efficient models. E2E features and optimisation.	Horizontal and vertical integration of IoT DT models. IoT DT that is capable of modelling and simulating the future state and behaviour of the IoT device.
IoT DT Modelling and Simulation Platforms	IoT DT platforms at the edge. Virtual sensing and actuation functions and simulations.	Predictive modelling platforms. Modelling and simulation of energy efficiency.	Integrated IoT platforms with virtual simulation environments including XR.
IoT DT Security	IoT DT security features integrated.	IoT DTs counterfeiting identification and mitigation.	Automatic recognition of fake DTs and their isolation or elimination.
IoT DT Connectivity	Simulation and modelling of the communication channels.	Define influence of the environments on the communication parameters of the IoT DTs.	Virtual platforms for the connectivity of IoT devices.

9. IoT Swarm Systems

Swarm intelligence for edge IoT systems deals with various IoT devices coordinated using self-organisation, decentralised and distributed control. It consists of simple autonomous edge IoT devices and agents that come as emergent collective intelligence.

Swarm intelligence addresses the area of IoT system collective behaviour and is inspired by social swarms in nature such as bird flocks, ant colonies and honeybees.

Swarm and edge computing combined with IoT are used to implement the collective behaviour of physical and virtual AI decentralised and distributed IoT systems.

From that concept new terms such as "artificial intelligence of things", "internet or intelligent things" are derived and are emerging to address collective intelligence in IoT systems with no centralised control infrastructure.

These new developments create new "Internet of Robotic Things", "Internet of Intelligent Mobile Things" and "Intelligent IoT Devices Colonies" applications that apply the principle of swarm and edge computing to fleets and groups of edge IoT devices, supporting an always increasing number of items as the technology improves.

9.1 Technological developments

The future edge IoT swarm systems bring fundamental research challenges in cross-domain IoT resource orchestration. For instance, in designing new multi-intelligent-agent-based edge IoT frameworks. Each IoT device could be associated in the future with an agent or a DT at the edge. The agents could utilise swarm intelligence to jointly optimise the operations and information flow for their respective IoT devices.

The move towards collective intelligence in edge IoT systems requires intelligent orchestrators for heterogeneous systems leading to swarm computing concepts.

To achieve that, new intelligent programming orchestrations for distributed and decentralised open architectures and methods for updating/upgrading over-the-air (OTA) IoT smart devices are required.

Collaborative functions ask for leveraging edge IoT swarm systems to improve network connectivity, enhancing information collection ability through each edge IoT device and intra-networking issues for a swarm of edge IoT devices.

The energy spent on edge IoT devices during swarm task execution is a key aspect to be considered. Total energy consumption includes static energy consumption and dynamic energy consumption during different tasks and the connectivity to other IoT devices and edge processing.

The development of collaborative edge IoT swarm systems raise the issue of vulnerability to attacks by hackers from other fleets or via the interface with the cloud. The inherent distributed architecture for edge IoT swarm systems makes them more robust and secure and implies that the information is shared, stored, exchanged, and analysed locally and inside the swarm fleet, making it harder for hackers to access sensible data.

The real-time processing and response of edge IoT swarm systems make it hard for malicious attackers to detect devices' sensitive information. '

The edge IoT systems interfaces to other edge-cloud infrastructure derive several security problems that have to be considered (swarm identity (ID) leakage, forgery, tampering, spam, jamming, swarm IoT device impersonation).

The distributed nature of edge IoT swarm systems require new efficient service discovery protocols to design such that IoT devices and users can identify and locate the relevant swarm services and providers to satisfy the application requirements.

Real-time optimisation protocols for edge IoT swarm systems are required as future mobile IoT applications are dynamic and involve using online edge resource orchestration capabilities and provisioning to continuously handle dynamic edge IoT swarm devices workloads and tasks.

The distributed edge computing architecture for edge IoT swarm systems shifts the research on how trust and security are addressed. The development of decentralised trust solutions with services provided by different secured and trustworthy edge IoT entities is part of the new E2E implementations.

New efficient security mechanisms for edge IoT swarm systems are required to ensure IoT device authentication, data integrity, and mutual IoT swarm platform verification and validation. New secure routing schemes and trust network topologies are key for edge IoT swarm systems.

The development edge IoT swarm systems must consider the balance between the HW and SW constraints for edge IoT swarm devices combined with the level of intelligence implemented in the edge devices and their connectivity capabilities to perform in a swarm fleet adequately. As a result, developing SW, HW, and AI-based algorithms for handling computation offloading from edge to the IoT swarm device is a critical issue to be addressed.

The inherent distributed architecture of future edge IoT swarm systems consider interoperability, collaboration as part of the system, and the platforms operating these systems include efficient algorithms to facilitate collaboration.

Edge IoT swarm systems may display a considerable level of heterogeneity in terms of IoT devices, level of intelligence, connectivity, and processing capabilities and, therefore, efficient IoT platforms that deal with this heterogeneity are highly desired.

The collaborative intelligent interaction among the IoT swarms requires further research on federated learning to execute or train ML models in edge IoT devices as part of a swarm fleet.

9.2 Main Trends, Issues and Challenges

The research in IoT edge swarm systems complements the traditional AI approach to cognition and combines individual reasoning, collaborative intelligence, and mobile and sensing intelligence.

The IoT swarm computing must address the interaction with the environment in which the swarm IoT fleets operate, including research concerning federated learning processes and simple perceptions of forms, recognition of other IoT devices, and the swarm fleets' interaction with other fleets and humans.

The evolution of mobile edge IoT fleets that mimic complex behaviours must consider the development of techniques to model and simulate the interaction of simple edge IoT devices, to explore psychological ideas and the nature of collaborative intelligence in mobile IoT fleets.

Research on expanding the concept of intelligent agents receiving real-time data combined with mesh computing applied to IoT edge swarm systems can support the advancement in collaborative intelligence for edge IoT.

Edge IoT swarm-based intelligence assumes that a group of IoT swarm devices or intelligent agents can perform tasks without explicit representations of the environment, and the IoT swarm devices or agents operate combining planning with reactivity.

The self-organisation of flow patterns in edge IoT swarms research is a challenge, especially in providing solutions for intelligent and efficient behaviour of the whole IoT swarm fleet when we combine the limited intelligence of the individual IoT devices.

Further research needs to study the essential elements of edge IoT swarm dynamics providing mechanisms for implementing such behaviours and HW, SW, algorithms for modelling, simulating, and integrating self-organisation agents into edge IoT devices.

One of the major challenges of edge IoT swarm systems is to encode and deploy the collective behavioural characteristics of a fleet of edge IoT swarm-based fleets into the behaviour of the individual edge IoT devices.

Research on complex adaptive behaviour is needed to provide HW, SW, and connectivity mechanisms to implement interactions between edge IoT devices as distinct from behaviour that directly results from the operations of individual edge IoT devices.

The advances in edge IoT swarm systems are directly linked with the research in providing optimised mechanisms and techniques for providing the ability to mobile IoT swarm devices to separate, cohere, align, and avoid obstacles.

Separation is the ability to operate with other IoT devices and keep a certain separation distance from different devices and avoid crowding too closely together in a fleet. The cohesion function allows the IoT devices to approach or form a group of edge IoT devices.

The alignment feature supports the devices to identify the expected next movement and synchronise the movements of IoT devices relative to each other.

Navigating and avoiding obstacles (e.g., perception and processing efficient collision detection algorithms) is another critical challenge to be addressed by research in IoT swarm-based fleets.

The work in edge IoT swarm systems must be combined with the latest advances in neuromorphic computing with edge IoT devices using neuromorphic HW and collaborative neuromorphic operating systems (OS).

The connectivity solutions in edge IoT swarm systems becomes critical in implementing collaborative intelligence. New ultra-low-power mesh communication protocols must be combined with neuromorphic architecture to provide self-X functions to edge IoT swarm systems.

A new approach to cognition must be considered for edge IoT swarm systems that include capabilities and mechanisms for remembering, forgetting, or continuous learning combined with search algorithms and strategies for performing exploratory analysis, interaction, communication, and exchanging information.

The research combining edge IoT swarms and AI opens the opportunities to address the evolutionary computing capabilities of edge IoT devices and predict the continuous evolution and transformation of the edge IoT swarm systems based on their missions and applications.

9.3 Research Priorities Timeline

Table 7 Swarm systems research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Swarm programming languages, tools, and OS	Define applicability and requirements of different swarm system, coming out with a taxonomy that help in Identifying different category of swarm.	Efficient implementation of languages, OS and tool for swarm managing and simulation.	Coherent and homogeneous Integration of SW and tool that allow to treat swarm fleets as a legacy IoT device in the full IoT-edge-cloud continuum
Domain applicability of swarms	Use case definition and Impact on verticals analysis.	Integration of swarms in multiple verticals sectors and demonstrate added value.	Swarms substitute in a seamless way for final users some of the currently existing IoT devices.
Swarms AI-fication	Applicability of traditional AI methods to swarm systems.	Implementation of advanced AI techniques in swarm system.	Full integration of cutting-edge AI technologies in swarm management.
Communication within and outside of the swarm	New low-power and very low latency protocols for in-swarm communication.	Smooth integration of delay sensitive networks surrounding the swarm with the in-swarm communication protocols.	Fluent, low latency and self-organizing communication of in-swarm and out-of-swarm protocols.

10. Internet of Things Senses

Internet of Things Senses (IoTS) is an aspect of the IoT paradigm, by which unique sensing technologies are applied to replicate over the Internet the senses of sight, hearing, taste, smell, and touch, facilitated by AI, VR/AR, intelligent connectivity, and automation.

IoTS developments are essential for IoT, considering the growing interest towards technologies related to the Metaverse[28], which require cognitive decision-making capabilities of the edge devices, thanks to the use of AI algorithms implemented into such devices (e.g., robotic things).

The IoTS technologies complete and expand the abilities and features of many edge IoT devices by including different senses, (e.g., the human senses plus mechanoreception-balance, temperature, and other ways to indicate situations in which an autonomous IoT device can be impeded to work, e.g., due to too high pressure or too high temperature) and equipping the edge devices with new perception mechanisms and experiences, by integrating augmented intelligence and information across senses, time, and space.

Digital sensory experiences introduced by IoTS provide new types of Human-Machine Interface (HMI) devices, replacing keyboards, mice, and joysticks by providing interactions with the senses, so to allow a radical re-shape of some industrial domains as well as new use cases and business models.

10.1 Technological developments

By the next decade, digital sound, and vision, complemented by the above-mentioned sensing technologies, will transform the current screen-based experiences into multi-sensory ones, practically indivisible from physical reality, as predicted by the Ericsson ConsumerLab report[29].

The report investigates what that could mean for consumers, with AR glasses as the entrance point. It presents what the consumers envisage as future developments driven by IoT sensory connectivity through AI, VR, AR, intelligent connectivity, and automation.

The development of IoTS is supported by advances in sensing, signal processing, low-power and sustainable devices, and edge analytics to detect, analyse and monitor the deployed sensing technologies.

Touch consists of several distinct sensations (e.g., pressure, temperature, light touch, vibration, and pain) that are integrated into tactile internet developments. For humans, touch feelings are part of the touch sense. They are attributed to different receptors in the skin, which are mimicked by sensors measuring the reaction to pressure, temperature, touch, vibration, etc. The Touch sense can be also used to allow bi-directional communication between IoTS devices and humans, for instance in case of blind and dumb people.

[28] Y. Wang et al., "A Survey on Metaverse: Fundamentals, Security, and Privacy," in IEEE Communications Surveys & Tutorials, 2022, doi: 10.1109/COMST.2022.3202047.

[29] Ericsson ConsumerLab, "10 Hot Consumer Trends 2030 - Internet of the senses", December 2019, Online at: https://www.ericsson.com/4ac661/assets/local/reports-papers/consumerlab/reports/2019/10hctreport2030.pdf

Sight is the ability to perceive items through the eyes that can be represented by different types of vision sensors, cameras, and AR glasses. Such devices can for instance sustain navigation, search for routes, identify places and recognise devices, objects, persons, and sights.

Smell can detect different odours/scents/aromas, which can be represented by sensors that focus on specific odours. The remote smell integrated as an online experience for humans and things can enhance the abilities of edge IoT devices to smell scents in remote environments, deliver new services and improve the perception in these environments.

Taste is the ability to sense tastes like salty, sweet, sour, bitter, and savoury. The different tastes can be detected by various sensors that provide a palette of tastes with a determined scale. Combining the information from the distinct taste sensors provides the experience of detecting a flavour.

Hearing is the ability to recognise and decode sound waves and vibrations. The detection of sound, e.g., by using different types of microphones and vibration sensors, enhances the edge IoT devices' capabilities, thanks to new or recently enhanced techniques, e.g., for voice control, voice biometrics, and automatic language translation.

In addition to the five standard human senses, one could consider in the IoTS domain an additional one, which is the sense of space (see **Figure 7**), based on merging and fusing the information from multiple sensor types and correlating them with the cognition process to better comprehend there surrounding environment where edge IoT devices are operating.

The sense of space is essential in the mobile autonomous edge devices operating in fleets across various environments. These edge IoT devices can use other sensors to deliver complex behaviours, for instance to detect movement for balance control, tilt the body of an object, and sense the direction and acceleration to attain and maintain equilibrium.

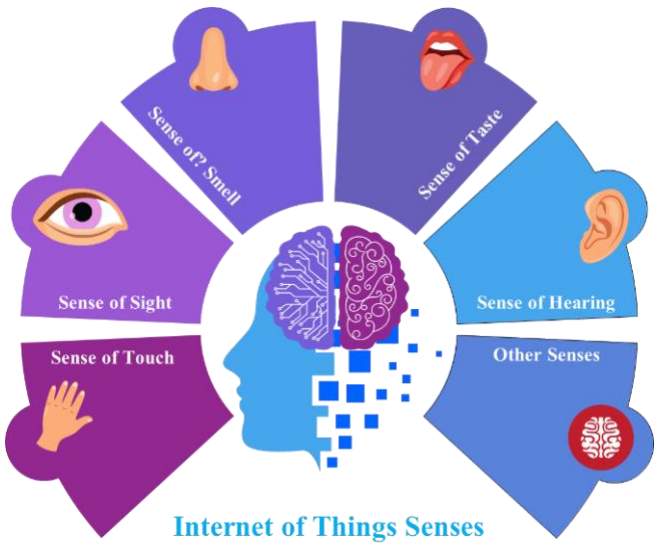


Figure 7 Internet of things senses

Moreover, the Tactile IoT paradigm[30] integrates ultra-low latency with extremely high availability, reliability, and security. It enables humans and machines to interact with their environment in real-time, using haptic interaction with visual feedback while moving and within a specific spatial communication range.

Finally, a new set of technologies and innovations are surfacing, all aiming at making a commercial reality the Metaverse, a topic on which attention is raising also in the European associations landscape, e.g., the new BDVA[31] activities related to the Metaverse, for which IoTs can be seen as a key enabling technology.

10.2 Main Trends, Issues and Challenges

The development of IoTS, including Tactile IoT, requires reliable, robust and intelligent connectivity solutions and new edge-ready software and hardware for quickly and seamlessly managing, storing, analysing, and accessing the huge amount of data produces by sensors.

Further research and development in hyperconnectivity are needed to take the metaverse, VR and AR to the next level for uniform video streaming and remote control/surgery, or tactile internet.

The current network infrastructure cannot support the emerging IoTS applications in terms of reliability, latency, cost and sensibility of sensors and actuators, access networks capabilities, system architecture and mobile edge platforms.

The design requirements of IoTS systems and devices to achieve real-time interactions are still dependent on the monitoring of the underlying system and environment, based on human (or human-like) senses limited by the perception processes.

Research in autonomous monitoring of IoTS systems and identification of real-time adjustments of the connectivity and processing parameters are needed to control and optimise the IoTS loop processes.

IoTS applications have ultra-low E2E latency and ultra--high reliability design requirements. They need to guarantee data security, availability, and dependability of systems without infringing the latency requirements and considering the encryption delays and the E2E processing loop.

Research on decentralised and distributed networks and IoT architectures based on mobile-edge computing and cloudlets is needed to advance both Tactile IoT and IoTS applications across industrial sectors.

Multidisciplinary research covering intelligent connectivity to increase bandwidth and capacity with the development of sensing and signal processing for 3D audio and holograms using volumetric video is also needed.

Further research on sense-based intelligent connectivity includes the feel, taste, and smell of digital objects replicas of physical edge IoT devices and the development of platforms that can model and simulate the merging of digital and physical worlds into one another.

[30] N. Promwongsa et al., "A Comprehensive Survey of the Tactile Internet: State-of-the-Art and Research Directions," in IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 472-523, Firstquarter 2021, doi: 10.1109/COMST.2020.3025995.

[31] Big Data Value Association (BDVA): https://www.bdva.eu/

Implementing the intelligent connectivity solutions demanded by IoTS applications require new research to address the efficient radio resource allocation in wireless/cellular networks due to multiple haptic, human-to-human (H2H), machine-to-machine (M2M), and machine-to-human (M2H) communications that have various and sometimes conflicting service requirements.

As haptic communications are bidirectional, symmetric resource allocation with the guarantee of a minimum constant rate in both the uplink and the downlink needs to be ensured.

The above-mentioned challenges that current networks face give raise to a set of requirements, which in turn bring new issues for managing and orchestrating the wireless/cellular network parameters to provide priority for resources based on QoS, safety and mission-critical features.

Spectrum issues need to be tackled as well, as the heterogeneity of access strata and bands used in the different vertical domains will require a holistic approach and a swift management of the existing bands, which are needed to deliver the flawless immersive experience required by IoTS services.

Finally, dynamic, and flexible resource allocation techniques across different protocol layers, including adaptive management and network slicing with on-demand functionality, are required for future edge IoT deployments.

10.3 Research Priorities Timeline

Table 8 Internet of things senses research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Sensors and Actuators	Development of haptic edge sensors and actuators with wireless mesh connectivity capabilities. Enhance the sensors capabilities in terms of precision, range, sensitivity, response time, spatial resolution, reliability, cost, and temperature dependence.	Research on lightweight energy-efficient, fast response time, low-cost, actuators providing capabilities of both the cutaneous and kinaesthetic feedback.	Development of new haptic actuators, cutaneous, muscle type for force tension, kinaesthetic, skin type for vibration, pressure, pain, temperature, etc.
Sensing Systems	Research on surface sensing using multiple arrays of sensors and techniques to identify the forces across the surface. New reading techniques for distributed sensing and actuation optimised for low-energy and acceptable latency.	AI-based sensor fusion techniques for multi-modal sensory. Real-time multiplexing schemes across protocol layers for integrating the various modalities in dynamically varying wireless environments.	Research on edge AI platforms for integration of multi-modal sensing systems for edge IoT applications.
Resource Managing and Orchestration	Further work on standardised groups of energy-efficient haptic codecs to be integrated into the kinesthetics and tactile information, to perform effectively in time-varying wireless environments. Development of new suitable performance metrics for analysing and comparing the performance (e.g., information fusion, connectivity features, data processing techniques, data reduction and control, compression, etc.) of various haptic systems over IoTs.	Research on the optimisation of collaborative multi edge IoT device communication and the effect of overlay routing, and IP-level routing on E2E latency. Research on ultra-high reliability in haptic communications considering trade-offs among reliability, latency, packet header to the payload ratio, etc.	Research on managing and orchestrating the wireless/cellular networks parameters to provide priority for resources based on QoS, safety-, mission-critical features for IoTS systems.

11. Decentralised and Distributed edge IoT Systems

New network architecture paradigms for the forthcoming intelligent connectivity era are driven by a decomposition of the architecture[32] into platforms, functions, orchestration, and specialization aspects.

Future network platforms will be associated with an open, scalable, elastic, and agnostic heterogeneous cloud, which is data flow centric, will include hardware acceleration options together with a heterogeneity of computing architecture (x86, RISC-V, ARM, etc).

11.1 Technological developments

For cellular connectivity, functionally, the convergence of RAN and CN, together with a broader adoption of the Open Radio Access Network (O-RAN)[33] concept, will help reduce architectural complexity.

At the same time, options of flexible offload, extreme slicing and flexible instantiation of sub-networks will drive the increased level of specialization of the architecture.

Of high relevance for the open provision of services and the monetization of resource will be the transformation of orchestration architecture; cognitive closed loop and automation are likely to become pervasive.

All future deployment scenarios will rely on a superior transport network and network fabric that is flexible, scalable, and reliable to support demanding use cases and novel deployment options, such as a mixture of distributed RAN and centralized/cloud RAN enabled by AI-powered programmability.

Other interesting directions are provided by intent-based networks[34] and semantic-based networks[35]. In any case, the future network architecture shall provide the capability to facilitate all the AI operations in the network.

The expansion of edge IoT applications will entail massive deployment of communicating objects. Administrators of these applications aim to deliver the required coverage for large networks with minimised energy consumption and without multiplying BSs.

Self-adaptive networks are needed, relying on IoT devices as relays. These micro networks would manage the flows of information from a heterogeneous set of communicating entities, e.g., IoT devices, robotic things, and sensors, locally interacting in a complex system.

5G standardisation assumes the forthcoming deployment of network slices and private networks, which are supposed to bring their own network nodes.

[32] Y. Xu, B. Qian, K. Yu, T. Ma, L. Zhao and H. Zhou, "Federated Learning Over Fully-Decoupled RAN Architecture for Two-tier Computing Acceleration," in IEEE Journal on Selected Areas in Communications, doi: 10.1109/JSAC.2023.3236003.

[33] A. Giannopoulos et al., "Supporting Intelligence in Disaggregated Open Radio Access Networks: Architectural Principles, AI/ML Workflow, and Use Cases," in IEEE Access, vol. 10, pp. 39580-39595, 2022, doi: 10.1109/ACCESS.2022.3166160.

[34] P. Lingga, J. J. Kim and J. P. Jeong, "Intent-Based Network Management in 6G Core Networks," 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2022, pp. 760-762, doi: 10.1109/ICTC55196.2022.9952437.

[35] X. Luo, H. -H. Chen and Q. Guo, "Semantic Communications: Overview, Open Issues, and Future Research Directions," in IEEE Wireless Communications, vol. 29, no. 1, pp. 210-219, February 2022, doi: 10.1109/MWC.101.2100269.

Here, micro-networks of potential different ownership and with a potentially external security management might share parts of the infrastructure with wide area networks, paving the way for a set-up where a private network with partly owned infrastructure and a private trust policy are integrated in a public network.

11.2 Main Trends, Issues and Challenges

Decision making and optimisation: taking into consideration an E2E system made of three elements, the edge, the network, and the cloud (where information flows from the edge through the network to the cloud and vice versa), critical issues are what are these decisions, and equally important, where do those decisions take place, with which implications on the overall network.

The main consideration is that any network is a complex entity, since it is distributed, heterogeneous in different aspects (data streams, computation, and storage capabilities, required QoS, etc.), time varying (in some but not all aspects), and resource limited.

The application of the decision theory to the more and more important problem of distributed resource allocation is still a hot research question that needs to be addressed[36].

What is looked for is a framework or model that would allow to decide where in a network (edge, cloud, intermediate stages?), both processing and decisions about resource allocation are made, and that does that in a way that is responsive in near real-time.

Research is needed in novel IoT distributed architectures to address the convergence of low latency, Tactile Internet, edge processing, AI and distributed security based on ledger or other technologies, and an effective deployment of multi-access edge computing (MEC).

Developing specific architectural requirements for distributed intelligence and context awareness at the edge is a future research topic, especially when considering the integration with mesh network architectures, so to form knowledge-centric networks for IoT, capable of serving many different applications coming from numerous vertical sectors.

Research on orchestration of IoT heterogeneous networks, adaptation of software defined radio and networking technologies for IoT, considering built-in E2E distributed security as well as hardware-based security solutions[37], trustworthiness, and privacy issues in edge computing environment must be extended, addressing the federation and cross-platform Integration for edge IoT applications.

[36] A. Mukherjee, P. Goswami, M. A. Khan, L. Manman, L. Yang and P. Pillai, "Energy-Efficient Resource Allocation Strategy in Massive IoT for Industrial 6G Applications," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5194-5201, 1 April1, 2021, doi: 10.1109/JIOT.2020.3035608.

[37] J. Gopika Rajan. and R. S. Ganesh, "Hardware Based Data Security Techniques in IOT: A Review," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 408-413, doi: 10.1109/ICOSEC54921.2022.9952021.

11.3 Research Priorities Timeline

Table 9 ***Decentralised and distributed edge IoT systems research priorities***

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Decision making	Partially distributed decision-making mechanisms and techniques. Federated sub-system sharing a common decision mechanism	Fully distributed decision-making methods. Federated systems of systems sharing the same decision mechanisms	Fully distributed and federated systems, using heterogeneous decision mechanisms targeted to specific QoS or vertical sectors.
Security aspects	Established Privacy preserving techniques. Block-chain based security methods applied to selected vertical sectors.	Scalable block-chain based security mechanisms addressing some vertical sectors. Trustworthy and auto-adapting communication among several vertical sectors.	Secure-by-design system of systems, endowed with swarm intelligence and hardware-based security measures, fully Decentralised security procedures, self-adapting to real-time demands of heterogenous actors.
Learning mechanisms	Distributed learning. Federated learning.	Distributed and federated learning.	Continuous learning, self-adapting to the dynamic changing environment of a heterogeneous network supporting several vertical sectors.

12. Federated Learning, Artificial Intelligence technologies and learning for edge IoT Systems

To perform according to the devised expectations[38], the new distributed IoT architectures for computing optimisation across the edge continuum need to improve responsiveness by reducing decision-making latency, to increase data security and privacy, to decrease power consumption, using less network bandwidth, thus maximizing efficiencies, reliability, and autonomy.

The IoT edge contains computing capabilities scaled across the micro-, deep- and meta-edge to process workloads, including the latest technology like AI model training and ML inference and signal processing, using signal conditioning[39] followed by neural networks[40] computing. The neural network computing and memory requirements are significantly reduced by using signal conditioning on the raw data.

In this context, federated learning as a distributed ML technique, which creates a global model by learning from multiple decentralised edge clients, is a significant technological development that can be implemented in distributed IoT architectures across the edge continuum.

Federated learning uses complex methods for handling distributed data training by enabling the cooperative training of common AI models, by combining and averaging locally calculated updates submitted by edge IoT devices. Federated learning permits training new models on multiple edge IoT devices simultaneously without the need to have data stored in a central cloud.

12.1 Technological developments

Integrating AI-based techniques across the edge continuum requires a new layer of edge processing infrastructure and scalable, energy-efficient modules for AI-based processing[41].

Federated learning methods offer several advantages, including scalability and data privacy, with ML and DL algorithms that can be executed on edge IoT devices, delivering faster real-time insights for increased IoT application efficiency. Bringing AI to the edge increase the efficiency of processing the data locally and reduces latency and the cost of connectivity for many IoT applications.

In the distributed data exchange environment, federated learning/training combined with the IoT heterogeneous compute based on various underlying processing architectures (CPUs, GPUs, NPUs, neuromorphic, etc.) can provide the solution for future IoT edge intelligent heterogeneous systems.

[38] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.

[39] R. Tirupathi and S. K. Kar, "Design and analysis of signal conditioning circuit for capacitive sensor interfacing," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 1717-1721, doi: 10.1109/ICPCSI.2017.8392007.

[40] Z. Li, F. Liu, W. Yang, S. Peng and J. Zhou, "A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects," in IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 12, pp. 6999-7019, Dec. 2022, doi: 10.1109/TNNLS.2021.3084827.

[41] Vermesan, O. and Nava, M.D. (Eds.). Intelligent Edge-Embedded Technologies for Digitising Industry. River Publishers Series in Communications, June 2022. ISBN: 9788770226110, e-ISBN: 9788770226103. Online at: https://www.riverpublishers.com/pdf/ebook/RP_E9788770226103.pdf

The federated learning/training must consider the underlying connectivity systems, including Bluetooth, Wi-Fi, LPWAN, mesh, 5G and beyond applied to the IoT application topology, range, and power requirements. The convergence of connectivity, AI/ML, and processing can ease the implementation of different IoT federated learning/training solutions for industrial and consumer applications.

The concept of IoT federated learning/training is combined with the IoT edge mesh, which allocates the decision-making tasks among edge devices within the network. The computation and processing tasks and data are shared using an IoT networks of edge devices, routers, PLCs, and micro-servers.

The IoT edge mesh combined with federated learning/training provide distributed processing, low latency, fault tolerance, scalability, security, and privacy, as required by IoT applications, which demand higher reliability, real-time processing, mobility support, and context awareness.

Cooperative IoT computing based on federated learning/training provides better usage of resources, reduced latency, due to easy access to local resources, better services, as IoT devices can cooperate to get better information, reduced communication with centralised entities, and improved security and privacy as data remain most of the time within a local network.

Enabling distributed intelligence in IoT/edge computing or swarm computing applications is difficult due to a set of known problems, e.g., synchronisation, consensus, cooperation etc. In addition, due to scalability and complexity issues of IoT systems, it is challenging to determine how to generate, coordinate and federate the intelligence, which edge IoT device provides intelligent functionality and how different edge IoT devices cooperate, transfer, and acquire intelligence.

12.2 Main Trends, Issues and Challenges

The challenge for many IoT applications is that federated learning/training uses multiple entities collaborating to solve ML problems under the coordination of a central server. This approach for edge networks creates many issues concerning security and privacy and the data itself.

Federated learning raises several risks and weaknesses in terms of computational complexity in the case of heterogeneous edge IoT devices that may have limited computing resources, inadequate wireless connectivity quality, or may use different OSs.

Another edge IoT federated learning challenge relates to communication delays expressed as the latency between edge IoT devices and the ML system. Decreasing latency is critical for AI-based edge IoT devices operating in real-time applications such as industrial equipment.

Replacing the client-server process of the federated learning/training model with fully decentralised learning replaces communication with the server by peer-to-peer communication between individual clients.

Optimisation algorithms are necessary to implement federated learning/training at the edge, considering edge IoT devices' constraints and resource limitations as part of the edge continuum.

The IoT devices limited bandwidth can restrain scalability, but this is solved in IoT edge mesh architectures, as data is sent to multiple edge IoT devices that share data with other devices. The communication bottleneck issue is resolved due to the distributed nature of the system.

At the same time, the computation tasks are offloaded to different edge IoT devices, operation which speeds up the processing time and increases the efficiency of federated learning/training, leading to better response time, reduced make span, and higher throughput. The distribution of loads drives the edge IoT systems to be more flexible and robust, as, in the case of a device failure, other devices can share the load of the failed IoT device.

IoT systems are dynamic, as devices can be mobile, added, removed, or changed in configuration; all of the above require new context-aware solutions for distributed security and privacy algorithms.

The heterogeneity of computing, communication and AI technologies requires AI-based algorithms that are portable across different IoT edge environments. Communication technology is intrinsically heterogeneous for what concerns data rate, transmission range, and bandwidth. The IoT SW solutions depend on the HW, and programming models are needed to execute workloads simultaneously at multiple HW levels.

Research on standard protocols and interfaces should address the integration of AI-based algorithms and lightweight protocols for communicating with different devices in a heterogeneous environment.

More research is needed to develop distributed learning/training algorithms and to maximise the average time between errors and optimise the availability by minimising the failure probability and average recovery time in the OTA learning/training process.

The IoT federated learning/training must consider the hybrid computing method that combines HW/SW and AI techniques across the edge continuum. Hybrid computing implies the integration of specialised advanced AI processors at different computing levels for both high-level and low-level operations.

Further research is needed to develop optimised algorithms for federated learning/training to complement and effectively leverage the computing capabilities with the AI-based processors and other types of processor architectures.

12.3 Research Priorities Timeline

Table 10 Federated learning and AI for edge IoT systems research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Federate learning approaches	Techniques and methods to integrate federated learning into IoT/edge computing systems. Management of edge IoT systems, by addressing mesh network security and management by leveraging ML. Research on central training data sets and edge IoT local data sets.	Edge IoT intelligence architectures and AI frameworks for federated learning. Development of tools and tool chains for dedicated edge IoT federated learning. Methods for providing reference training datasets for performing standard federated learning application tuning.	Benchmarking techniques and methods for edge IoT federated learning. Scalability and portability of AI-based models for federated learning across the edge granularity.
Federated learning architecture and frameworks	Advanced architectural approaches for the federated learning server integrated into mesh networking environments.	Extend the capabilities of open-source federated learning frameworks. Communication and computation efficiency of the federated learning architectures, synchronisation optimisation among edge IoT devices.	Federated learning architectures addressing task scheduling, dynamic resource allocation to achieve low-latency services.
Hardware platforms for federated learning	HW requirements for implementing federated learning in edge IoT computing environments.	HW heterogenous solutions to minimise memory transfer, increase energy efficient and improve computational speed. Computation offloading and content caching using dynamic cache allocation techniques, context-aware offloading algorithms adapted to resource-constrained (e.g., limited storage and capacity) edge IoT devices.	HW/SW/AI algorithms heterogeneity management. Understanding of the effect of system heterogeneity on the AI model aggregation efficiency, accuracy and the divergence or convergence of optimisation processes.

13. Operating Systems and Orchestration Concepts for edge IoT Systems

The extension of the IoT edge and edge-cloud federation is redefining the use of OSs and orchestration concepts across the IoT-edge-cloud continuum in real-time applications.

The increased use of embedded systems combined with processing units at the edge requires new ways of virtualising the computing capabilities and the OSs across the diversity of the HW components at the IoT edge. This also requires more frequent updates and upgrades of FW, SW, algorithms, and security patches for edge IoT devices. Challenges arise with more functions and services implemented in FW/SW/algorithms and the increasing complexity of electronic component interoperability, including managing agile and vulnerable edge IoT devices.

13.1 Technological developments

The development of ubiquitous meta-OSs[42] to provide an integration framework that implements processing and a better traceability, safety, and security across the IoT edge must consider several challenges. Ubiquitous meta-OSs for IoT edge applications must embed features and functions to allow the applications to be autonomous, cooperative, situational, evolvable, and trustworthy.

As the heterogeneity of edge IoT increases, edge IoT devices need to act with a valid secure method, both using centralised and distributed intelligence. The developments of ubiquitous meta-OSs for IoT edge applications are not yet ready to ensure scalability and provide the functionalities and capabilities that would allow Billions of edge IoT devices to work independently of each other and cooperate in real-time.

Among the biggest challenges for ubiquitous meta-OSs for IoT edge applications one can mention how to effectively provide real-time features to applications and OS capabilities to heterogeneous edge IoT devices, and how to interact with federated platforms and interface with cloud provider agnostic solutions. Building supporting platforms would have a substantial impact in providing solutions to those issues.

The challenges for autonomous orchestration of distributed edge systems are related to maximising utilisation while assuring the Service Level Objective (SLO) of workloads running at resource constraint edges and dealing with inhomogeneous/heterogeneous platforms at the IoT edge.

The above-mentioned challenges need to address critical features, like network slicing, that open for an entirely new set of use cases. For example, given a set of network slices, how do we assure that each one will hit Its performance targets while at the same time not over-provisioning resources at large. Overall, the orchestration needs to become more autonomous and lift the burden of Site Reliability Engineers (SRE) running the systems to date.

Artificial Intelligence Operations (AIOps) and Machine Learning Operations (MLOps) techniques and methodologies could form the basis for genuinely autonomous systems at the edge.

[42] P Trakadas, et Al., "A Reference Architecture for Cloud–Edge Meta-Operating Systems Enabling Cross-Domain, Data-Intensive, ML-Assisted Applications: Architectural Overview and Key Concepts", in Sensors 2022, 22(22), 9003; https://doi.org/10.3390/s22229003.

The heterogeneity of IoT edge brings a paradigm shift towards application-driven components and systems, interoperability, and open-source HW, SW solutions. There is a strong need for a data strategy and establishing trusted data exchange frameworks across OEMs, system integrators, and component vendors.

Mission- and safety-critical real-time edge IoT applications require guaranteed latency and bandwidth, the integrity of data, security, resilience, and controlled mesh networking. Ubiquitous meta-OSs for IoT edge applications can act as orchestrators that aggregate and compose services according to users' requirements and coordinate their execution in a coherent and smart way.

Ubiquitous meta-OS for IoT edge and orchestrating methods are needed to simplify the development, orchestration, and security of distributed IoT edge architectures and solutions. The development of new solutions using at the edge containers, virtual machines, and unikernels[43] provides a flexible foundation for expanding distributed edge computing deployments with a choice of heterogeneous HW, applications, and federated edge-clouds infrastructures. This brings further challenges to ensure distributed firewall, open orchestration APIs, support for virtual machines, containers, and unikernels application deployment models.

13.2 Main Trends, Issues and Challenges

New research and key innovations are needed to address orchestration in the future. For instance, novel interfaces between the legacy IoT architecture and the new one will be required. This will allow users to exploit innovations in the control planes (e.g., moving from centralised systems to more decentralised ones) and new HW features in heterogeneous (from the compute capability point of view) platforms, so to be able to place mission-critical workloads at the edge.

OSs and orchestration concepts for decentralised and distributed edge IoT systems are needed to provide an integrated environment for the next-generation intelligent IoT applications. Such applications embed IoT in distributed computing systems operating in a continuum at the edge across micro- deep-, meta-edge and are interfaced and federated with the cloud solutions. IoT/edge computing platforms and the new IoT applications can create new business models relying on meta-OS orchestration, distributed edge intelligence, storage, and resources heterogeneity.

Ubiquitous meta-OSs for IoT edge and orchestrating mechanisms are required for heterogeneous systems with lightweight virtualisation, virtual machines, microservices and containers. Key issues to be addressed are data pre-processing at the edge, edge analytics, scalability, efficiency, dependability, trustworthiness, adaptability, and transparency. The issues are even more critical considering the evolution of IoT towards Tactile IoT and IoTS.

Research activities must solve several critical technical challenges, including the availability of a distributed architecture of ubiquitous meta-OSs, scalability, performance and applicability issues, self-X features, and autonomous considerations.

Ubiquitous meta-OSs developments for IoT edge must align with the emerging new computing paradigms such as IoT swarm, including intelligent robotics things, organic computing, broad usage of AI, and neuromorphic concepts.

[43] http://unikernel.org/

The development of new SW-defined abstractions and capabilities for edge IoT devices is needed to support the management, application development, and communications between devices across the edge and cloud continuum.

Context-awareness in the edge IoT system is related to the context information, the real-time operation and the dynamicity of processing, scalability and managing the information with the support of the ubiquitous meta-OS.

Research should address the issue of creating a flexible context modelling framework to provide means of presenting, maintaining, sharing, protecting, reasoning, and querying context information. In this context, the IoT edge meta-OS must include adaptability and self-X features to allow the IoT application to adapt its behaviour according to the context. The IoT system can then be reconfigured to adapt to these context changes.

Self-X functions, including self-organising, self-healing, self-protecting, self-diagnosing, self-reconfiguring, require a form of self-awareness to understand the state of the edge IoT system and are to be embedded into the meta-OS, which must realise its state and configuration, and the state and the configuration of the resources it controls and manages.

Research in developing models of edge IoT HW and ubiquitous meta-OS-level SW configuration is necessary to describe the topologies and the rationale for the designs of IoT devices and their integration into the distributed IoT edge applications architecture. The development of new software-defined abstractions and capabilities for edge IoT devices is needed to support the management, application development, and communications between devices across the edge and cloud continuum.

The meta-OS features for IoT edge require adapting to the characteristics of these future applications that will be context-sensitive, adaptive, customised, and reconfigurable. The functional requirements behind the concepts of IoT systems reconfigurability, context-awareness, adaptability, and customisation mean that the meta-OS supports and allows that the IoT system's HW and SW configurations can seamlessly change at runtime.

13.3 Research Priorities Timeline

Table 11 Operating systems and orchestration concepts for edge IoT systems research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Decentralization techniques	Mature federated learning techniques that provide clear advantages in selected verticals and use cases	Advanced federated learning techniques suitable for all verticals	New paradigm of distributed management
Context awareness	Understanding the key surrounding parameters and functionalities that can guarantee an advance context awareness	Context awareness improved with semantic capabilities, i.e., abstracting from the sheer heterogeneous data and going up in the abstraction layer	New context awareness paradigm
Operating Systems	New meta-OS that can proof advantages against existing traditional OSs	Enhanced distributed meta-OSs that adapt resource computation and storage allocation to the run-time environment on a ms scale	Fully autonomous and reconfigurable management of the system resources in the IoT-edge-cloud continuum with fully distributed decision capabilities

14. Dynamic Programming Tools and Environments for Decentralised and Distributed IoT Systems

Current programming environments and tools for IoT[44] provide a centralised approach (either on-premises or cloud-based) where the main component transforms and processes most of the computation on data supplied by the edge and far edge devices.

This approach unfortunately implies several drawbacks, for instance unused edge computational power, a single point of failure, and violation of data boundaries (private, technological, etc.).

In this context, new research is needed in leveraging the resources available in lower-tier devices to improve overall dependability, performance, scalability, observability, and reproducibility of IoT systems using new programming and tools for distributed IoT.

14.1 Technological developments

Extensive edge IoT distributed systems are difficult to implement. Programming these systems is challenging due to the requirement to assert numerous control paths resulting from the innumerable interleaving of messages and failures, produces by a huge number of heterogeneous devices.

The edge IoT distributed systems developments need to consider the integration of lightweight meta-OSs, distributed databases, middleware, mesh networking, and application architecture types. This means addressing the design and analysis of distributed algorithms, programming languages, compilers, SW tools and dynamic middleware environments.

Managing edge IoT distributed systems infrastructure requires dedicated sets of programming tools.

The dynamic programming tool for coding, modelling, simulating, and visualising the current operational state of all edge IoT devices, including verification and validation components and debugging and testing modules notifying when the failure occurs in the distributed IoT systems.

The edge IoT distributed systems bring inherent challenges such as concurrency, partial failure, node dynamism, or asynchrony in their design and implementation.

The increasing complexity of the concurrent activities and reactive behaviours in edge IoT distributed systems are unmanageable by the existing programming models, tools, and abstraction mechanisms.

14.2 Main Trends, Issues and Challenges

The research should consider transforming and decomposing data flow and partitioning of data exchange between the distributed IoT nodes while detecting current conditions in deciding when to move computations along the edge continuum.

[44] A recent survey of the most used tools can be found at: https://www.iotforall.com/top-iot-tools-and-platforms-for-iot-development-and-developers.

The decomposition into heterogeneous IoT distributed environments needs to be done based on a selected decomposition schema.

New techniques such as graph representations can provide an unambiguous computation model to abstract the application definition from its architecture to achieve a specific level of decentralization and heterogeneity. Infrastructure-independent application definition is needed that only contains data processing logic.

The execution should be achievable on different sets of IoT devices with other capabilities using several algorithms for flow decomposition. The development of programming tools must integrate elements to design and evaluate mechanisms for component deployment and dependency management.

The edge IoT devices of a complex distributed system can evolve heterogeneously, therefore exhibiting diverse component configurations. In these conditions, mechanisms are required to resolve and deploy component dependencies upon installing new components on the edge IoT devices.

The research activities in the following years must consider solving several issues that are part of the edge IoT systems development, such as failure detection and partitioning of the system, replication and consistency, storage, and processing.

The research in edge IoT distributed systems requires new techniques for the integration, management, and interoperability of distributed data, methods, technologies, services, architectures, applications, and interfacing with legacy IoT systems.

The heterogeneous integration of wireless communications (cellular, Wi-Fi, LPWAN, etc.), mobile, ad-hoc, mesh networks, and sensors as part of complex edge IoT distributed systems require addressing novel algorithms, uses, and implications of distributed concepts, models, architectures, technologies, and deployments.

Future work in this area requires exploring various representation techniques like semantics[45], meta-data, tagging[46], ontologies[47], and knowledge bases[48] applied to edge-distributed environments.

The evolution of edge IoT distributed systems towards collaborative creation, resource sharing, and problem-solving requires combining the theory of distributed systems and technologies with parallel processing concepts and integration with cognitive-based[49] algorithms.

Testing and debugging edge IoT distributed systems are inherently complex and need to address many aspects, ranging from performance testing through scalable and accurate network emulation, correctness testing and debugging the edge IoT distributed systems.

[45] C. Dong, et Al., "Semantic Communication System Based on Semantic Slice Models Propagation," in IEEE Journal on Selected Areas in Communications, vol. 41, no. 1, pp. 202-213, Jan. 2023, doi: 10.1109/JSAC.2022.3221948.

[46] H. Jang, et Al. "IoT Device Auto-Tagging Using Transformers," 2020 12th International Conference on Advanced Infocomm Technology (ICAIT), Macao, China, 2020, pp. 47-50, doi: 10.1109/ICAIT51223.2020.9315384.

[47] C. -Y. Huang, Y. -H. Chiang and F. Tsai, "An Ontology Integrating the Open Standards of City Models and Internet of Things for Smart-City Applications," in IEEE Internet of Things Journal, vol. 9, no. 20, pp. 20444-20457, 15 Oct.15, 2022, doi: 10.1109/JIOT.2022.3178903.

[48] Y. Shen, et Al., "Prior Knowledge based Advanced Persistent Threats Detection for IoT in a Realistic Benchmark," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 3551-3556, doi: 10.1109/GLOBECOM48099.2022.10000811.

[49] A. Giuliano, et Al., "A Review of Cognitive Dynamic Systems and Cognitive IoT," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 2022, pp. 1-7, doi: 10.1109/IEMTRONICS55184.2022.9795834.

The programming tools for building and testing edge IoT fault-tolerant distributed systems must include these elements to address these complex challenges.

14.3 Research Priorities Timeline

Table 12 Dynamic programming tools and environments for edge IoT systems research priorities

TOPIC	SHORT TERM	MEDIUM TERM	LONG TERM
	2023-2024	2025-2027	2028-2030
Programming tools	Programming tools for distributed algorithms for solving dynamic programming problems and work on models for asynchronous distributed computation addressing energy efficiency.	Tool chain techniques for edge IoT systems including formalisms and programming models. Enhance the language support for implementation, specification, and systematic testing of asynchronous edge IoT systems.	State machine-based programming language that supports the dynamic features required for building edge IoT asynchronous systems.
Integrated development environments	Integrated development environments and tools using module-based compositional refinement elements for development reasoning of dynamic edge IoT distributed systems.	Evolution of the development environment for edge IoT distributed systems to include the design of efficient, AI-based components, support for DLTs, swarm and mesh networking using mechanisms for addressing the heterogeneity of these systems.	Integrated development environments to address the dynamic changes in architectural patterns, abstractions, and component models for network-partition-tolerant, scalable, elastic, and self-X edge IoT distributed systems enabling testing and debugging.
Distributed system environments	Monitoring solutions for distributed edge IoT systems, including scanning how the data is collected, processed, distributed, and presented following what events are available and measuring the required parameters for the distributed processes.	Lightweight, agentless approaches and solutions for built-in monitoring technologies and protocols integrated into edge IoT distributed systems. Explore new hybrid and data streams approaches for monitoring distributed edge IoT systems.	Development programming models and protocols for reconfigurable edge IoT distributed systems.

15. Heterogeneous Edge IoT Systems Integration

The next-generation IoT and edge systems are evolving towards heterogenous and hybrid systems, integrated using various technologies. IoT and edge computing heterogeneous system integration is essential for providing IoT solutions that offer scalability, security, and resilience for IoT application needs.

Heterogeneous edge IoT system integration refers to the integration of various HW/SW/AI components and convergence of different technologies into a higher-level IoT system that provides enhanced functionality and improved operating characteristics.

The IoT applications require the integration of heterogenous technologies including sensors, devices, edge processing, and the cloud, with a variety of protocols and standards for communication. All these require certificate based E2E security to improve the overall robustness of the proposed products.

Edge IoT heterogeneous systems comprise sensors, computing units, interconnects, processing, memory, connectivity, SW, and AI modules. The compute units can be very different, ranging from CPU, GPU, ASIC, DSP, ASSPs, FPGAs to SoCs. Different interconnects (e.g., PCIe, Ethernet) connect all these compute units.

Each memory hierarchy of these computing units accesses these memories in a specific manner. The SW modules have usually to support different OS, virtual machines, runtime libraries and compiler toolchains.

In edge IoT heterogeneous systems, memory bandwidth and data transfer between each compute unit can be unbalanced, and the different computing units have their own programming models, making integrating these systems difficult.

15.1 Technological developments

The edge IoT distributed systems are a result of technology convergence that enables the enhancement of edge IoT at the device, system, and application levels.

Several technologies, such as identification technology, IoT architecture technology, communication and network technology, network discovery technology, computing, AI, discovery and search engine technology, SW and algorithms, sensors and HW technology, power and energy storage technology, data and signal processing technology, network management technology, security and privacy technologies, and standardisation are contributing to the functionality of the edge IoT systems.

IoT heterogeneous system integration involves ecosystems of IoT connected devices, applications, and systems, including sensing, communication, processing, data analytics, enterprise-user apps, and a platform to streamline operations. All these components need to communicate seamlessly without compromising the quality or the performance of the overall E2E system.

In the context of edge IoT systems, there is a need to define a heterogeneous system architecture with specifications for integrating various sensors, processing units, SW and HW components, AI frameworks, and connectivity. The goal is to make the IoT heterogeneous devices compatible from an IoT system-level perspective.

IoT heterogeneous system integration aggregates disparate devices, protocols, and enterprise systems for seamless operations, to provide E2E solutions interacting with IoT factory application integrators to connect IoT devices to the backend.

This requires a deep knowledge domain and understanding of technologies and implementations to establish enterprise-wide connectedness systems across IoT architectural layers and industrial applications, aligned with the enterprise functions.

As the number of IoT devices increases, the architectures evolve towards distributed systems, the complexity of IoT deployment expands significantly.

Edge IoT system integration requires interdisciplinary skills, work experience, proper planning, and vital ecosystems to cover the entire process, from design and development to deployment and maintenance.

IoT heterogeneous system integration implies the selection of IoT platforms that allows the storage, processing, sharing and visualization of the captured data by the distributed IoT devices, flexibility in managing content and permissions, and processing the data across the edge-cloud continuum, while allowing an easy use of the APIs, which can be focused on different kind of system integrations.

15.2 Main Trends, Issues and Challenges

The heterogeneity of edge IoT distributed systems (e.g., protocols, device data format, communication capabilities of the devices, technologies, HW, platforms, intelligence) creates a challenge to the large-scale implementation and scalability of edge IoT distributed systems.

Several levels of heterogeneous integration can be identified for edge IoT systems. The heterogeneous integration starts at the components level, which includes the sensors, microcontrollers, analytics, and communication modules as part of the IoT device level.

Next, there is heterogeneous integration at the SW and AI framework levels. And on the top, there is heterogeneity at the edge IoT system level. Heterogeneity at all levels leads to edge IoT system reconfigurability.

Different platforms have been developed for edge IoT heterogeneous integration, including sensors, circuits, SW, processing, AI, and communication technologies.

However, deploying these platforms requires edge IoT solutions covering the whole scale, from sensors and devices, through efficient circuit design, SW, and AI technologies to novel system-level architectures and methodologies.

Integrating heterogeneous devices allows for raising the processing capacity of edge IoT devices. Integrating edge IoT systems (software, HW, AI, training datasets, etc.) create System of Systems (SoS) solutions that can improve the features of IoT applications.

15.3 Research Priorities Timeline

Table 13 Heterogeneous edge IoT systems integration research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Heterogenous HW solutions	Power-efficient performance for heterogenous HW including neural processing units (NPUs), to enable highly flexible, efficient processing for specific workloads and increased code portability across processors and platforms.	Reliable SW across the edge, fog, and cloud processing for heterogenous edge IoT HW systems.	Hybrid HW heterogeneous system architecture for edge IoT integrating heterogeneous processing elements into a coherent processing environment.
Heterogenous integration	Integration concepts to combine the heterogeneity of devices, data formats, communication, and interoperability issues due to heterogeneity.	Define frameworks for continuous design and validation flows for edge IoT heterogeneous systems.	HW/SW co-design on the next-generation intelligent, adaptive, and autonomous edge IoT systems.
Models	Modelling techniques for heterogeneous edge IoT systems considering models for physical phenomena, architecture, computation, communication scheduling, self-awareness, and adaptation.	Methods and techniques to model the edge IoT systems and their topology, heterogeneity, system loads, and simulation tools to identify how these parameters influence the system performance.	Simulation integration (co-simulation) of edge IoT heterogeneous systems by addressing scaling, composition, extensive range of required time resolution, HW-in-the-loop simulators and increasing automation in simulation integration.

16. Edge IoT sectorial and Cross-Sectorial Open Platforms

The IoT platforms are categorised considering the area of operation and the functionalities (e.g., device, connectivity, edge, cloud), the sector (e.g., industrial, consumer, business), or the openness (e.g., open-source, commercial, proprietary) they address.

The IoT platforms developed around specific IoT devices or components provide the features for implementing functions to secure that the connected devices are installed, configured, and maintained using regular FW/SW updates and upgrades.

The IoT platforms focusing on connectivity provide capabilities and features for connecting various IoT devices to support, manage and orchestrate the connectivity functions, and implement communication services.

16.1 Technological developments

The edge IoT platforms are developed to provide advanced capabilities near the edge of the network close to the IoT devices that collect data or deliver processed information.

The edge IoT platforms that implement the management capabilities for implementing a distributed architecture required to exchange data among the edge IoT devices integrated into the edge IoT platforms, are required to use HW-agnostic scalable architectures to support the deployment of functions across the edge continuum covering micro-, deep- and meta-edge.

Cloud-based IoT platforms are centralised solutions implemented by cloud providers to support developers to create and deploy IoT solutions on their clouds (e.g., IaaS, PaaS). Many of these platforms offer advanced AI-based analytics and offer tools including ML and other AI techniques to secure actionable insights from IoT data.

Edge IoT platforms help facilitate localised processing on edge IoT devices to support analysing data streams, including information about networks, actions, and other infrastructure the edge IoT devices are connected to or interacting with.

Edge IoT platforms deliver containerised components that are deployable on IoT devices, runtime modules to execute actions locally at the edge, and interfaces with other edge or cloud platforms using, in many cases, cloud-based interfaces for monitoring and management.

The edge IoT platforms embed IoT analytics to the edge to increase processing efficiency and security by reducing the amount of data being transferred over networks so that processing can be completed locally on edge IoT devices.

The industrial, consumer, business edge IoT platforms are developed to provide IoT solutions for the specific economic sectors, and they are in many cases tailored for the specific need in these sectors.

The industrial edge IoT platforms are created to match the industrial manufacturing requirements to monitor edge IoT devices, process the data series, event streams, support and convert a variety of industry open or proprietary protocols, interpret data at the edge or in the cloud and provide analytics on industrial data collected.

The industrial IoT platforms provide an integration framework for IT and OT systems facilitating data sharing and consumption for the integration of new real-time asset management.

The next-generation edge IoT platforms require a move from specific vertical industrial sectors to horizontal IoT platforms that implement distributed architectures based on edge computing capabilities operating across several industrial sectors.

Such platforms need to integrate several connectivity and processing technologies, advanced analytics and data management capabilities that enable developers to easily design and deploy IoT solutions faster, accelerating time to insight for applications operating across several industrial sectors.

16.2 Main Trends, Issues and Challenges

Specific research challenges for next-generation edge IoT platforms are to address the issues of heterogeneity, scalability and federated learning (FL) by implementing distributed architectures that guarantee the security and privacy of the data exchanged by an extensive number of intelligent edge IoT devices while subduing interoperability issues.

The research advances in the area of cognitive cloud platforms require new solutions for the federation of edge IoT platforms and the orchestration of edge-cloud domains for optimising the use of the resources, improving service quality, reducing the energy, the inefficient flow of data, and the costs.

Further research is needed to address the technological and semantic interoperability issues among heterogeneous IoT devices and platforms in the context of implementing distributed architectures and the integration of new technologies such as swarm computing.

The research needs to focus on minimising the complexity of collecting and processing vast amounts of real-time data generated by intelligent IoT devices, address scalability and security issues.

The increased focus on IoT solutions built using open-source SW and HW, which are based on open specifications allowing portability and reducing IoT applications development, require further research on open-source technologies.

The research and innovation priorities must address the convergence of technologies for edge IoT platforms combining the technological development in a long list of areas, e.g., sensing, processing, communication, computing, AI, and storage technologies.

The research priorities need to support the development of new open, edge IoT horizontal platforms combining the distributed functions for mobile edge computing and the interfaces to synergize and federate with other edge or cloud platforms.

The advances in intelligent industrial IoT applications, Tactile IoT and autonomous/robotic systems solutions require real-time response and computing at the edge of the networks and FL across the edge.

New research is required to provide AI algorithms to operate in a heterogeneous distributed IoT application context, including a federation of edge IoT and cloud platforms.

AI and IoT FL advances require new development frameworks to enable the effective development of edge IoT platforms embedding AI-based components at different IoT architectural layers.

Further development of edge IoT platforms needs to support the creation of intelligent, self-X functions (e.g., self-organising, self-healing, self-configuring, self-managing) integrated into the platforms to deal with the intelligent autonomous IoT and swarm systems.

These functions include SW/HW and AI-based algorithms that enable automated tasks (e.g., to create, provision, configure, troubleshoot) that manage fleets of IoT devices and gateways securely, remotely, in volume or individually.

Various AI techniques, rule engines, event stream processing, data visualisation and ML need to be developed to address the micro-, deep, and meta-edge and integrated into the IoT platforms.

The IT and OT security measures and features must be considered and developed in the context of distributed architecture and across the edge-cloud continuum.

The advances in IoT/edge computing need to address secure data storage, efficient data retrieval and dynamic data collection as part of a processing framework for IoT along the computing continuum considering the functions of data pre-processing, storage and analytics based on both edge and cloud computing infrastructures.

16.3 Research Priorities Timeline

Table 14 Edge IoT sectorial and Cross-Sectorial Open Platforms research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Simulation capabilities	Edge IoT platforms can simulate and run a IoT devices in a specific vertical domain	Edge IoT platforms across multiple IoT verticals domains and supporting partial twinning.	Edge AI platforms working and seamless simulating all industrial domains and make use of advanced twinning.
Interoperability among platforms	Each edge IoT platform has its own API to expose its services to the outside world	Edge IoT platforms that can exchange data among themselves, making use of the recently defined data spaces at European level.	Edge IoT distributed platforms with embedded AI capabilities applied to industrial sectors and use Research on advanced edge AI platforms to exchange abstract data sets and make use of all defined data spaces at the European level.
Convergence of technologies	Edge IoT platforms that combine distributed architectures converging mesh, DLT and AI technologies.	Advanced edge IoT AI-based platforms with integrated cognitive functions for federated learning and other emerging distributed learning technologies.	Advanced edge IoT platforms including digital twining technologies to address the metaverse continuum for novel immersive applications.

17. IoT Verification, Validation and Testing (VV&T) Methods

The broad range of existing security certification schemes for products, systems, domains, solutions, services, and organizations derives on a heterogeneous environment of solutions, making it difficult to understand what is needed to achieve a certain level of security in each context or technology. This heterogeneity also makes comparing certified devices more difficult, especially when different certification approaches, countries, and contexts are used. Currently, there is no unified solution that copes with these problems, facilitating the process of comparing and assessing the security levels.

17.1 Technological developments

Due to the dynamism of security defined by the new vulnerabilities discovered, affecting the security or the change of the domain that have different security requirements (e.g., IoT devices that passes from a medical to a home domain), the certification approach must adapt to these changing conditions. An agile certification process is required to ensure such security level is up to date during the lifecycle of a device. In addition, the approach must cope with the business requirements and needs of the market. It means that security certification approaches should be efficient and cost-effective, so the market product launch is not delayed.

17.2 Main Trends, Issues and Challenges

While pure functional verification of IoT systems still poses challenges, e.g., due to HW/SW integration issues, AI at the edge, and the distributed nature of IoT systems, verifying non-functional properties, such as cybersecurity or resource consumption, usually is at least as challenging. Also, integrating untrusted third party IoT devices in sensitive or safety-critical systems often comes with the challenge to prove the absence of hidden "unwanted" functionality (e.g., backdoors), which can go as deep as needing to employing techniques like binary code analysis.

The edge IoT distributed, heterogeneous systems employ multi-languages for implementation or for services edge IoT devices provide. Distributed systems use different forms of concurrent programming that increase HW concurrency and sources of heterogeneity.

Developing reliable, safe, and secure edge IoT distributed systems is a trade-off process that must be able to also scale among the different level of performance that are needed in the different configurations.

The development requires novel models, logical notations, verification techniques, extensions, improvements, and combinations of existing ones to catch the behaviour of such systems and ensure that they meet various specific requirements. In this context, advanced formal methods applied to the verification and validation of edge IoT concurrent and distributed heterogeneous systems can provide new understandings of the efficiency of these methods, when compared with other approaches. Given the financial pressure on IoT device development, any verification activity must be cost effective and efficient, hence, the automation of verification tasks is an important trend. Cost and efficiency of verification also is heavily linked to the proper usage of design methodologies like "security-by-design", as rigorous design will significantly cut down testing efforts.

Verification of non-functional properties like cybersecurity lags behind functional verification, even if the former can have even bigger financial risk attached.

Research shall focus on new and improved methods for the automated verification of non-functional HW/SW properties of IoT systems. In addition, the functional verification of edge IoT AI-based solutions, which is a largely open challenge, must be addressed.

Verification research on edge IoT system should consider virtual environments (incl. digital twins), and design approaches promising greater efficiency at reduced error - and vulnerability rate into account. This may include formal development/rigorous design, low-code/model-based and other approaches. Finally, investigating automating and improving the scalability of verification approaches for third-party "black-box" systems, which look at the HW and binary SW level of IoT systems, is required.

The heterogeneity of edge IoT distributed systems makes deploying and managing these systems complex. The distributed architecture of these systems adds to the complexity, as the IoT systems are deployed across networks and spatial boundaries.

Distributed systems display a high level of concurrency, which is a challenge in estimating the consistency and correctness of these systems, mainly when their behaviours are not appropriately defined. In the edge distributed systems, IoT devices become reactive systems, constantly interacting with the environment, and adjusting their states.

The distributed environment and the changing behaviour of edge IoT devices drive the IoT applications to be very dynamic and, therefore, exposed to unexpected behaviour. Identifying unexpected behaviour and assuring that the demanded behaviour is followed can create a challenge in dynamic systems. Intended behaviours in edge IoT distributed systems can be defined as properties. Model-checking techniques are used to see whether these properties hold onto the formal specification of the system. In this context, property specification, verification and virtual validation can help detect errors in edge IoT dynamic and distributed systems.

Further research must consider upcoming technologies such as HW/SW neuromorphic and swarm computation. Of further interest is the automation and integration of the design/verification/debug cycle with operational data: automated repair, diagnosis, and updates for systems in the field based on observed failures.

17.3 Research Priorities Timeline

Table 15 IoT Verification, Validation and Testing Methods research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Edge IoT AI-based systems VV&T	Virtual validation of edge IoT based system including AI-based components.	VV&T of self-X behaviours (e.g., self- configuration, self-healing, and self-adaption, etc.) of edge IoT systems.	Development of VV&T methods and techniques for real time and time constrained AI-based edge IoT distributed systems.
Distributed systems VV&T	Validation methods for edge IoT distributed systems focusing on both proof-based verification and systematic testing.	Mesh networking systems integrated as part of edge IoT infrastructure.	Edge IoT distributed systems embedding digital twin solutions.
Heterogenous systems VV&T	HW/SW neuromorphic and swarm computation applied to edge IoT distributed systems.	Heterogenous IoT distributed systems comprising of DLT platforms, edge AI frameworks and various ML implementations.	Federation of multi-blockchain-based data processing, edge IoT computing and swarm intelligence. Heterogenous edge IoT interoperability testing.

18. IoT Trustworthiness and Edge Computing Systems Dependability

Trustworthiness of the edge IoT systems can be defined as the degree of confidence one has that the edge IoT system performs as expected. Designing IoT edge trustworthiness into edge IoT systems requires the identification of characteristics and mechanisms of trust that can be embedded into the edge IoT system.

Trust in edge IoT systems is realised at the intersection of several dependability characteristics, as shown in **Figure 8**. As a result, trust in an edge IoT system is a concept with multiple dimensions, combining dependability characteristics with human and machine behaviour. In this context, there is a need for a greater understanding of how individuals interact with edge IoT devices and how edge devices interact with other devices/things concerning the extension of trust.

18.1 Technological developments

The dependability[50] of a system reflects the user's degree of trust in that system. Dependability characteristics applied to edge IoT systems are safety, security, reliability, resilience, availability, connectability, and maintainability as illustrated in **Figure 8**.

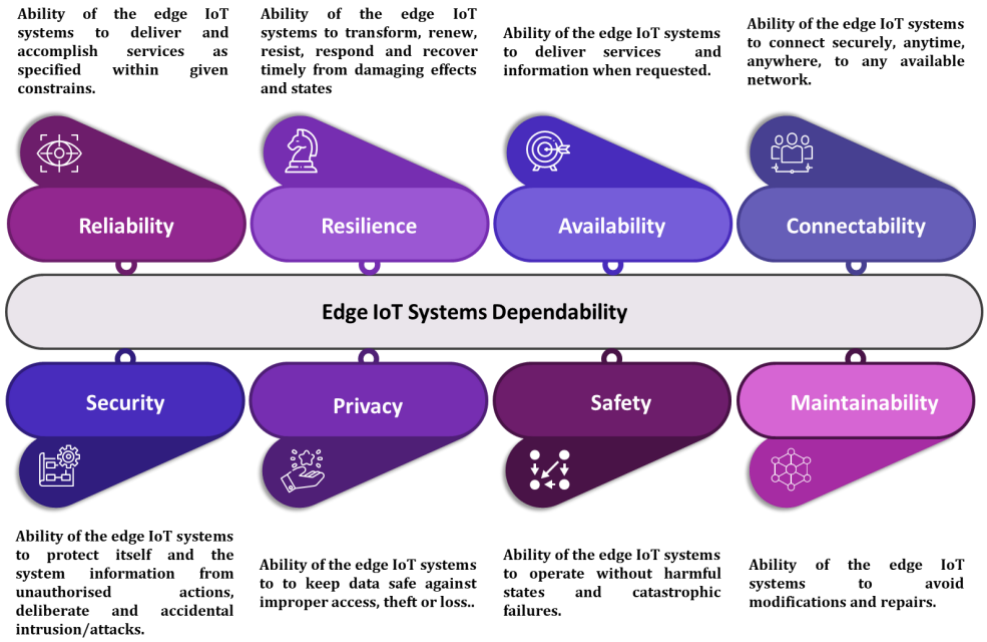


Figure 8 Edge IoT system dependability characteristics

The security aspects for IoT are critical due to the amount, diversity, and potential impact of security threats on everyday critical infrastructures. Security aspects represent one of the most pressing barriers to the adoption of large-scale IoT deployments.

[50] Laprie, JC. (1995). Dependability — Its Attributes, Impairments and Means. In: Randell, B., Laprie, JC., Kopetz, H., Littlewood, B. (eds) Predictably Dependable Computing Systems. ESPRIT Basic Research Series. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-79789-7_1.

Recent cyberattacks, such as the Mirai[51] or BrickerBot[52] IoT Botnets[53], highlight the need to design appropriate protection mechanisms for the next generation of IoT devices.

To address cybersecurity concerns, one of the most ambitious initiatives in Europe is the definition of a cybersecurity certification framework. In this direction, the recent "Cybersecurity Act"[54] represents the European Commission effort to strengthen the European Union Agency for Network and Information Security (ENISA)[55] role for the definition of this framework by providing additional guidelines and challenges for its realization.

The definition of a cybersecurity framework requires efforts from different knowledge domains to satisfy the requirements and needs of various stakeholders, such as manufacturers, institutions, legal firms, and consumers.

On the one hand, the very broad range of existing security certification schemes for products, systems, domains, solutions, services, and organizations derives on a heterogeneous environment of solutions, making difficult understanding what is needed to achieve a certain level of security in each context or technology.

This heterogeneity also makes comparing certified devices more difficult, especially when these devices are certified with different certification approaches, countries, and contexts. Currently, there is not a unified solution that copes with these problems, facilitating the process of comparing and assessing the security level.

On the other hand, due to the dynamism of security (e.g., a new vulnerability discovered affecting the security or a change of domain such as a device that passes from a medical to a home domain, implying different security requirements), the certification approach must consider these fast-changing conditions, which could affect the device's security level.

IoT Trustworthiness requires integrating stakeholders of the critical sector (network operators, technology suppliers, cybersecurity solution providers, standard and certification bodies, etc.) for defining cybersecurity standards and test procedures.

18.2 Main Trends, Issues and Challenges

With IoT devices taking over critical tasks in system control and/or health areas, dependability is one major trend: data provided must be reliable and trustworthy.

Dependable edge IoT systems will incorporate devices and services of multiple different vendors which will only increase the challenge. For example, such systems need to cope with data privacy, cybersecurity, reliability, and safety at the same time.

Without proper standards and planning, guaranteeing all these attributes over a set of diverse devices from different vendors (being deployed in different networks and data centres) is next to impossible.

[51] G. Tatebatake and S. Yamaguchi, "Mathematical Modeling and Analysis of the Dictionary Attack Mechanism in IoT Malware Mirai," 2022 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), Yeosu, Korea, Republic of, 2022, pp. 1-5, doi: 10.1109/ICCE-Asia57006.2022.9954838.
[52] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84, 2017, doi: 10.1109/MC.2017.201.
[53] R. Raman, "Detection of Malware Attacks in an IoT based Networks," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2022, pp. 430-433, doi: 10.1109/I-SMAC55078.2022.9987253.
[54] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.
[55] https://www.enisa.europa.eu/

Dependability management over the complete product lifecycle will become key and include techniques such as AI-augmented DevOps, safety and security-by design, dependability architectures, low-code development, code-re-use, and proper security management over the whole product lifecycle.

In a more technology-dependent world, cybersecurity concerns have attracted an increasing interest from companies, regulatory bodies, and end users. With the IoT, such aspects are exacerbated due to the amount, diversity, and potential impact of security threats on everyday critical infrastructures. Indeed, nowadays, security aspects represent one of the most important barriers for the adoption of large-scale IoT deployments.

Therefore, an agile certification process is required to ensure such security level is up to date during the lifecycle of a device. In addition, the approach must cope with the business requirements and needs from the market. It means that security certification approaches should be efficient and cost effective, so the product launch in the market is not delayed.

As a result of this process, a cybersecurity label is looked for, which contains the security level achieved by the device. It should provide a clear visibility of the level of security achieved but also give a non-ambiguous and complete representation of the results of the cybersecurity evaluation process.

This is rather difficult to achieve, because in comparison to the energy label, which measure a physical quantity, the measurement of security is far more complex, involving several security properties or dimensions. In addition, the label should be able to show in real time the security offered by the device.

The IoT and edge computing systems have challenges in addressing the automated cybersecurity evaluation towards a more agile and cost-effective certification, dealing with the IoT dynamism.

Finally, there is also the need for objectives and evidence-based evaluation methodologies that would allow for a homogeneous evaluation, including comparability aspects. This limits the security management mechanisms addressing the whole lifecycle of the IoT device, dealing with the security changes that might invalidate the certificate.

18.3 Research Priorities Timeline

Table 16 IoT Trustworthiness and Edge Computing Systems Dependability research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Trustworthiness	Edge IoT trustworthiness of ML models and explainability of AI (XAI) models used in Federated Learning.	Trustworthiness models for edge IoT self-adapting systems based on digital twin and AI-based technologies.	Frameworks providing guidelines, good practices and standards oriented to end-to-end trust in edge IoT systems.
Dependability	Define methods and tools to support the dependability system properties definition, composition and validation and relate the properties to different standards addressing different technologies.	Dependability properties at different layers of the edge IoT architecture by considering scalable concepts for HW, SW, connectivity, AI algorithms (inference, learning) and the design of flexible heterogeneous architectures that optimise the use of computing resources and the use of resource-constrained devices.	Virtualisation and simulation tools for managing the evaluation of edge IoT system dependability.
Benchmarking	Define different benchmarking methods and techniques of trust for an edge IoT system and provide compliance to an agreed-upon standard via certification schemes.	Benchmarking heterogenous edge IoT systems based on DLT, digital twins, mesh networking and AI technologies.	Benchmarking reference data sets for training edge IoT systems for federated learning.

Contributors

Editors:

Ovidiu Vermesan, SINTEF

Valerio Frascolla, Intel

Reviewer:

Damir Filipovic, AIOTI Secretary General

Contributors:

Alessandro Liani, Video Systems, Italy

André Bourdoux, IMEC, Belgium

Antonio Skarmeta, Universidad de Murcia, Spain

Antonio Soriano Asensi, Universitat de Valencia, Spain

Asbjorn Hovsto, Hafenstrom, Norway

Charles Sturman, Huawei, UK

Cian O Murchu, Tyndall National Institute, Ireland

Daniela Buleandra, SIMAVI, Romania

François Fischer, FSCOM, France

George Suciu, BEIA Consult International SRL, Romania

Georgios Karagiannis, Huawei, Germany

Ignacio Lacalle, Universitat Politecnica de Valencia, Spain

Ilia Pietri, Intracom Telecom Solutions, Greece

Jara Pascual, Collabwith Group, Netherlands

Jesus Angel Garcia Sanchez, Indra Sistemas

Joachim Hillebrand, Virtual Vehicle Research, Austria

Juho Pirskanen, Wirepas, Finland

Konstantinos Loupos, Inlecom, Greece

Konstantinos Thivaios, NETCOMPANY INTRASOFT, Luxembourg

Lazaros Karagiannidis, Institute of Communication and Computer Systems, Greece

Luis Munoz, University of Cantabria, Spain

Luis Perez-Freire, Fundacion Centro Tecnoloxico de Telecomunicacions de Galicia, Spain

Marcin Plociennik, Poznan Supercomputing and Networking Center, Poland

Marco Gonzalez Hierro, IKERLAN, Spain

Mario Drobics, AIT Austrian Institute of Technology GmbH, Austria

Martin Serrano, Insight SFI research Centre for Data Analytics, Ireland

Maurizio Spirito, Fondazione LINKS, Italy

Mikel Larranaga, Fundacion Tekniker, Spain

Mirko Presser, Aarhus University, Denmark

Monica Florea, SIMAVI, Romania

Natalie Samovich, Enercoutim, Portugal

Oltion Xhezo, Vodafone, UK

Ovidiu Vermesan, SINTEF, Norway

Pedro Maló, UNPARALLEL Innovation, Portugal

Pedro Ruiz, Integrasys, Spain

Philippe Sayegh, Verses Global, Netherlands

Pierre Yves Danet, 48deg79min-Consulting, France

Pieter Becue, IMEC, Belgium

Pietro Dionisio, Medea, Italy

Ranga Rao Venkatesha Prasad, Technical University Delf, Netherlands

Ricardo Vitorino, Ubiwhere, Portugal

Roumen Nikolov, Virtech, Bulgaria

Roy Bahr, SINTEF, Norway

Rute Sofia, fortiss, Germany

Sean McGrath, University of Limerick, Ireland

Sergio Gusmeroli, Politecnico di Milano, Italy

Srdjan Krco, DunavNET doo, Serbia

Valerio Frascolla, Intel, Germany

Veronica Quintuna Rodriguez, Orange, France

Acknowledgements

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT and Edge Computing Innovation in Europe, bringing together small and large companies, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share, and promote best practices in the IoT and Edge Computing ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT and Edge Computing Innovation in society. AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT and Edge Computing ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability, and defining policies.