

## D1.4

# Continuous technology watch and alignment

<b>WORKPACKAGE</b>	WP1	<b>PROGRAMME IDENTIFIER</b>	H2020-ICT-2020-1
<b>DOCUMENT</b>	D1.4	<b>GRANT AGREEMENT ID</b>	957246
<b>REVISION</b>	V1.0	<b>START DATE OF THE PROJECT</b>	01/10/2020
<b>DELIVERY DATE</b>	31/07/2023	<b>DURATION</b>	3 YEARS

© Copyright by the IoT-NGIN Consortium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 957246



## DISCLAIMER

This document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of its content.

This document may contain material, which is the copyright of certain IoT-NGIN consortium parties, and may not be reproduced or copied without permission. All IoT-NGIN consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the IoT-NGIN consortium as a whole, nor a certain party of the IoT-NGIN consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered using this information.

## ACKNOWLEDGEMENT

This document is a deliverable of IoT-NGIN project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957246.

The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

<b>PROJECT ACRONYM</b>	IoT-NGIN
<b>PROJECT TITLE</b>	Next Generation IoT as part of Next Generation Internet
<b>CALL ID</b>	H2020-ICT-2020-1
<b>CALL NAME</b>	Information and Communication Technologies
<b>TOPIC</b>	ICT-56-2020 - Next Generation Internet of Things
<b>TYPE OF ACTION</b>	Research and Innovation Action
<b>COORDINATOR</b>	Capgemini Technology Services (CAP)
<b>PRINCIPAL CONTRACTORS</b>	Atos Spain S.A. (ATOS), ERICSSON GmbH (EDD), ABB Oy (ABB), INTRASOFT International S.A. (INTRA), Engineering-Ingegneria Informatica SPA (ENG), Robert Bosch Espana Fabrica Aranjuez SA (BOSCHN), ASM Terni SpA (ASM), Forum Virium Helsinki (FVH), ENTERSOFT SA (OPT), eBOS Technologies Ltd (EBOS), Privanova SAS (PRI), Synelxis Solutions S.A. (SYN), CUMUCORE Oy (CMC), Emotion s.r.l. (EMOT), AALTO-Korkeakoulusäätiö (AALTO), i2CAT Foundation (I2CAT), Rheinisch-Westfälische Technische Hochschule Aachen (RWTH), Sorbonne Université (SU)
<b>WORKPACKAGE</b>	WP1
<b>DELIVERABLE TYPE</b>	[REPORT (Document, report, excluding the periodic and final reports)]
<b>DISSEMINATION LEVEL</b>	[PUBLIC (Public, fully open, e.g., web)]
<b>DELIVERABLE STATE</b>	[FINAL]
<b>CONTRACTUAL DATE OF DELIVERY</b>	31/07/2023
<b>ACTUAL DATE OF DELIVERY</b>	01/08/2023
<b>DOCUMENT TITLE</b>	Continuous technology watch and alignment
<b>AUTHOR(S)</b>	EBOS (Marios Sophocleous), ASM (Marco Antonio Bucarelli), ATOS (Jesus Gorroñoigoitia Cruz), ENG (Antonello Corsi), BOSCH (Jose Garcia Ontalba), I2CAT (Josep Escrig Escrig), AALTO (Yki Kortensniemi), SU (Serge Fdida)
<b>REVIEWER(S)</b>	ENG (Antonello Corsi), BOSCH (Miguel Urias Martinez)
<b>ABSTRACT</b>	SEE EXECUTIVE SUMMARY
<b>HISTORY</b>	SEE DOCUMENT HISTORY
<b>KEYWORDS</b>	Technology watch, survey, novelties, technology comparison

## 1. Document History

Version	Date	Contributor(s)	Description
V0.1	31/03/2023	EBOS	TOC
V0.2	30/06/2023	EBOS	Contribution to Chapters 1, 2, and 3 including assignment of chapters for each partner.
V0.3	05/07/2023	ATOS, EBOS, ASM, ENG	Contribution to Chapters 4 & 5
V0.4	17/07/2023	EBOS, ENG, BOSCH	Contribution to Chapter 3, executive summary and formatting
V0.5	28/07/2023	BOSCH, ENG, AALTO, SYN, ATOS, ASM, EBOS, I2CAT	Reviews and proof-reading
V1.0	01/08/2023	EBOS	Final version after addressing reviewers' comments

PENDING EC APPROVAL

## 2. Table of Contents

1. Document History	4
2. Table of Contents	5
3. List of Figures	7
4. List of Tables	9
5. List of Acronyms and Abbreviations	10
6. Executive Summary	11
1 Introduction	12
1.1 Intended Audience	12
1.2 Relations to other activities	12
1.3 Document Overview	13
2 IoT Technology Watch Survey	14
2.1 Survey Questions	14
3 Survey Results	20
3.1 Survey Analysis	20
3.2 Survey Conclusions Summary	30
4 Continuous Technology Watch	32
4.1 Technologies Identified for the 4 Verticals	32
4.2 Opportunities Identified for the 4 Verticals	33
4.2.1 Smart Cities	33
4.2.2 Smart Agriculture	34
4.2.3 Smart Industry	35
4.2.4 Smart Energy/Grid	37
5 Comparison of IoT-NGIN technological outcomes and other next generation IoT technologies	39
5.1 Enhancing IoT Underlying Technology	39
5.2 Enhancing IoT Intelligence	45
5.3 Enhancing IoT Tactile & Contextual Sensing/Actuating	50
5.4 Enhancing IoT Cybersecurity & Data Privacy	56
5.5 List of IoT-NGIN Technological outcomes	61
5.6 IoT Technological Maps & Direct Comparison to IoT-NGIN Outcomes	66
5.6.1 Enhancing IoT Underlying Technology	66
5.6.2 Enhancing IoT Intelligence	68

5.6.3	Enhancing IoT Tactile & Contextual Sensing/Actuating	71
5.6.4	Enhancing IoT Cybersecurity & Data Privacy	73
6	Conclusions	76
7	References	77

PENDING EC APPROVAL

### 3. List of Figures

Figure 1: Question 1: What industrial/technological sector is your company in? .....	14
Figure 2: Question 2: Please rank the following barriers to innovation in your industry with respect to the usage of IoT devices/systems.....	15
Figure 3: Question 3: What is your company's/institute role within the IoT ecosystem? ...	15
Figure 4: Question 4: What is your personal role within the IoT ecosystem? .....	16
Figure 5: Question 5: What are the key opportunities for IoT systems in the next 2-5 years? .....	16
Figure 6: Question 6: What do you think are the most relevant applications? .....	16
Figure 7: Question 7: What is preventing the adoption/growth of IoT systems at the moment in your industry segment? .....	16
Figure 8: Question 8: State 3 main pains, negative situations or risks for your entity with respect to the current IoT systems. ....	17
Figure 9: Question 9: State the 3 main gains or positive impact that you would like to see implemented in IoT systems in the next five years. ....	17
Figure 10: Question 10: What IoT technologies are you using right now? .....	17
Figure 11: Question 11: What are the IoT technologies you plan to use in the next 5-10 years? .....	17
Figure 12: Question 12: Order the following benefits by importance considering the needs of your industry segment. ....	18
Figure 13: Question 13: What kind of IoT related service would you use? .....	18
Figure 14: Question 14: What kind of options are you using in terms of edge and cloud solutions and why? .....	19
Figure 15: Question 15: Is your company using digital twins for asset management? .....	19
Figure 16: Question 16: Is there any deployment and installation timeline for a standard IoT ecosystem integration on a real industrial environment? .....	19
Figure 17: Question 17: Is there any initial cost evaluation of standard IoT ecosystem integration based on technologies defined? .....	19
Figure 18: Question 18: Is there any time period estimation for return of investment in deployment of standard IoT ecosystem? .....	19
Figure 19: Results from Question 1. ....	20
Figure 20: Results from Question 2: Please rank the following barriers to innovation in your industry with respect to the usage of IoT devices/systems. ....	21
Figure 21: Results from Question 3. ....	22
Figure 22: Results from Question 4. ....	22
Figure 23: Results from Question 5. ....	23

Figure 24: Results from Question 6. ....	23
Figure 25: Results from Question 7. ....	24
Figure 26: Results from Question 8. ....	25
Figure 27: Results from Question 9. ....	25
Figure 28: Results from Question 10. ....	26
Figure 29: Results from Question 11. ....	26
Figure 30: Results from Question 12: Order the following benefits by importance considering the needs of your industry segment. ....	27
Figure 31: Results from Question 13. ....	28
Figure 32: Results from Question 14. ....	28
Figure 33: Results from Question 15. ....	29
Figure 34: Results from Question 16. ....	29
Figure 35: Results from Question 17. ....	30
Figure 36: Results from Question 18. ....	30
Figure 37: Technological Map on the Enhancement of IoT Underlying Technologies. ....	67
Figure 38: Technological map on the Enhancement of IoT Intelligence. ....	69
Figure 39: Technological map on the Enhancement of IoT Tactile & Contextual Sensing/Actuating. ....	72
Figure 40: Technological map towards the Enhancement of IoT Cybersecurity & Data Privacy. ....	74



## 4. List of Tables

Table 1: List of identified technologies.....	32
Table 2: Functionalities vs baseline technologies for WP2 - Enhancing IoT underlying technology. ....	40
Table 3: Functionalities vs baseline technologies for WP3 - Enhancing Intelligence. ....	46
Table 4: Functionalities vs baseline technologies for WP4 - Enhancing IoT tactile and contextual sensing/actuating.....	51
Table 5: Functionalities vs baseline technologies for WP5 - Enhancing IoT Cybersecurity and data privacy.....	57
Table 6: List of IoT-NGIN Technological Outcomes. ....	61
Table 7: Main technological advancements towards the enhancement of IoT Underlying Technology.....	68
Table 8: Main technological advancements towards the enhancement of IoT intelligence.....	70
Table 8: Main technological advancements towards the enhancement of IoT tactile & contextual sensing/actuating.....	73
Table 10: Main technological advancements towards the enhancement of IoT Cybersecurity & Data Privacy.....	75

## 5. List of Acronyms and Abbreviations

IoT	Internet of Things
WP	Work Package

PENDING EC APPROVAL

## 6. Executive Summary

This document constitutes Deliverable “D1.4: Continuous technology watch and alignment”, which is the final output of Work Package (WP) 1, entitled “Next Generation IoT Requirements & Meta-Architecture but more specifically, Task 1.4 entitled “Continuous technology watch and alignment on Next Generation IoT advancements”.

This document focuses on the following outcomes:

- Implementation methodology, development and publishing of the IoT Technological survey
- Analysis of the IoT Technological survey results and the conclusions drawn from the obtained contributions
- A comprehensive list of identified IoT technologies from the continuous technology watch within the 4 verticals of IoT-NGIN and beyond
- A direct comparison of the identified IoT technologies with the technological advancements achieved within IoT-NGIN providing a clear differentiation for better exploitability of IoT-NGIN's Key Exploitable Results
- 4 IoT Technological Maps, one each technological field that IoT-NGIN advanced the state-of-the-art, showing in a graphical way the scientific and practical impact as well as positioning the project's outcomes in the IoT market.

The opportunities and challenges identified from the questionnaire, together with the list of IoT Technologies within the 4 verticals of the IoT-NGIN and beyond, have been blended into the technological maps of the 4 technological fields of IoT-NGIN namely, Enhancement of Underlying IoT Technologies (WP2), Enhancing IoT Intelligence (WP3), Enhancing IoT Tactile & Contextual Sensing/Actuating (WP4) and Enhancing IoT Cybersecurity & Data Privacy (WP5).

In addition to the technological maps, the direct comparison between the developed technologies and the state-of-the-art provided within this deliverable, provides a major stepping stone towards the exploitation and business model activities within WP8.

# 1 Introduction

The main objective of this deliverable is to report the newest advancements in next generation IoT technologies and show how these can be mapped and aligned with IoT-NGIN's outcomes. This deliverable is the next and final version of the work presented in D1.3 on the technology watch snapshot and identification and verification that the use cases trialed within IoT-NGIN are indeed the most relevant having the highest commercialization interest and potential amongst the targeted vertical industries.

Another objective of this deliverable is to present the technological survey developed and distributed to several IoT Hubs and communities, as well as other relevant research projects, whilst further provide the analysis of the results in an attempt to better understand the sectoral needs and opportunities for IoT-NGIN, with an initial focus on the involved vertical industry segments (i.e., smart cities, smart energy, smart agriculture and industry 4.0).

Moreover, the aim of this document is to provide information obtained through the technology watch and the outcomes of the technology-development WPs of IoT-NGIN in order to position IoT-NGIN's work on the relevant technological maps seeking to understand how IoT-NGIN project outcomes compare and contrast to other next-generation, IoT technological solutions being developed within the market. These maps and comparisons will be used as input to the exploitation and business model activities (T8.2 & T8.3) in WP8, to define a market position and unique value propositions for the solution.

## 1.1 Intended Audience

The document is particularly beneficial to end-users within the four verticals of smart agriculture, smart cities, smart energy, and industry 4.0. This document offers valuable information from both a technological and commercial standpoint, presenting significant advantages to these users.

For IoT stakeholders, considering the adoption of the newly aligned IoT-NGIN meta-architecture, the document could prove exceptionally valuable. It provides insights into architectural patterns relevant to their respective fields of interest, catering to IoT and edge hardware manufacturers, IoT solution providers, as well as 5G and AI-related stakeholders. Moreover, the entire Consortium can benefit from it for validation and exploitation purposes.

## 1.2 Relations to other activities

This document takes input from multiple tasks and WPs. Input is taken from WP1 and more specifically from Task 1.4 focusing on the continuous technology watch and alignment. Within Task 1.4, a technological survey was developed and distributed to a number of IoT Hubs and communities in order to identify the verticals with the most interest with respect to IoT technologies, as well as identifying challenges and opportunities for the IoT community in general and IoT-NGIN project specifically.

Significant input is taken from all the technology development WPs (WP2, WP3, WP4 & WP5). The technological advancements in the state-of-the-art stemming from those WPs was drawn and compared with the rest of the IoT technologies identified through the technology watch from Task 1.4. Input was also taken from D1.3, which provided a summarized version of the technological novelties of IoT-NGIN as well as the initial snapshot of the technology watch from Task 1.4.

Finally, this document provides input to the Impact Creation & Outreach WP (WP8), especially towards the exploitation and business models activities of the project (T8.2 & T8.3) to define the market position of IoT-NGIN's technological outcomes. To add to that, the document includes a direct comparison of IoT-NGIN's technological outcomes and the current state-of-the-art leading to the generation of 4 technological maps that significantly contribute to the proper definition of unique value propositions for the developed technologies and solutions.

## 1.3 Document Overview

The present deliverable is divided into six chapters, as follows.

In **Chapter 1**, the **motivation** and **objectives** of the deliverable are presented. Additionally, the chapter delves into the **connections with other Work Packages** within the project.

**Chapter 2** is dedicated to the **methodology and implementation of the IoT technological survey**. The survey consisted of 18 questions, from which some were multiple choice, some ranking and some open questions.

**Chapter 3** focuses entirely on a detailed **analysis on the obtained contributions**. Finally, a **summary of the conclusions drawn from the questionnaire** is presented at the last subsection of this chapter.

**Chapters 4** is a **summary of the identified IoT technologies** from the continuous technology watch, **within the 4 verticals chosen by IoT-NGIN**. It also shows some technologies that are relevant but not specifically for the 4 verticals. This chapter is essentially a comprehensive summary of the continuous technology watch snapshot from D1.3.

**Chapter 5** provides a **direct comparison of the identified IoT technologies** from chapter 4 and the **technological outcomes of IoT-NGIN**. It further presents 4 **technological maps** for the 4 main technological fields covered by IoT-NGIN showing the **contribution of IoT-NGIN towards the technological advancements in the respective fields**.

**Chapter 6** concludes with the **main findings and outputs of the report**.

## 2 IoT Technology Watch Survey

Within the framework of Task 1.4, a technological survey was created with a total of 18 questions:

- 8 open questions
- ranking questions
- 8 multiple choice questions

The questionnaire has as an aim and objective to understand the sectoral needs and opportunities for IoT-NGIN, with an initial focus on the involved vertical industry segments (i.e., smart cities, smart energy, smart agriculture and industry 4.0). An analysis of this questionnaire presented in the next chapter seeks to understand how IoT-NGIN project outcomes compare and contrast to other next generation IoT technological solutions being developed within the market. It is clear that with only 22 contributions, only exploratory research or insight can be obtained however, an initial comparison with the solutions in the market has been attempted.

The questionnaire was created using the EU Survey [1] service and was (still is) published on this link (<https://ec.europa.eu/eusurvey/runner/f4093771-3f77-15bf-e773-bee19abdefb4>). The questionnaire was advertised on all IoT-NGIN's social media and a pop-up was added to the website to fill it in. Furthermore, the questionnaire was distributed to several IoT-related hubs and communities, such as AIOTI, 5G-PPP, BDVA, and NGL, whilst it was further advertised to other relevant research projects and direct partners of the consortium. The questionnaire has finally received 22 anonymous contributions.

### 2.1 Survey Questions

As mentioned above, the questionnaire consisted of 18 questions, each one serving a different purpose. The 1<sup>st</sup> question shown below (Figure 1) aimed to confirm whether the 4 verticals chosen by IoT-NGIN were in fact the highest interest amongst the IoT community. Additionally, it intended to identify any other verticals with significant interest increasing awareness of the consortium towards other verticals. When the option "other" was chosen, a text field would show up for the contributor to add their working vertical.

\* Question 1: What industrial/technological sector is your company in?

- ☐ Smart Cities
- ☐ Smart Energy
- ☐ Smart Agriculture
- ☐ Industry 4.0
- ☐ Other

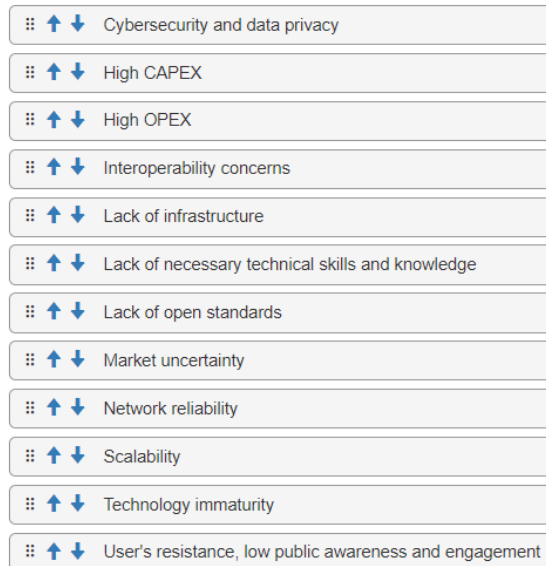
Figure 1: Question 1: What industrial/technological sector is your company in?

The 2<sup>nd</sup> question below (Figure 2) was meant to rank the most important challenges towards the implementation of IoT solutions in any industrial/technological sector. 12 challenges/barriers were included in the list with the assumption that those were the most important ones. However, an open text was also included at the end of this question allowing the contributors to mention any additional barriers in their industry, if any. This

## D1.4 - Continuous Technology Watch and Alignment

question further aimed to help the consortium understand the sectoral needs and opportunities for IoT-NGIN work within the specific verticals.

\* Question 2: Please rank the following barriers to innovation in your industry with respect to the usage of IoT devices/systems.  
Use drag&drop or the up/down buttons to change the order or accept the initial order.



:: ↑ ↓ Cybersecurity and data privacy
:: ↑ ↓ High CAPEX
:: ↑ ↓ High OPEX
:: ↑ ↓ Interoperability concerns
:: ↑ ↓ Lack of infrastructure
:: ↑ ↓ Lack of necessary technical skills and knowledge
:: ↑ ↓ Lack of open standards
:: ↑ ↓ Market uncertainty
:: ↑ ↓ Network reliability
:: ↑ ↓ Scalability
:: ↑ ↓ Technology immaturity
:: ↑ ↓ User's resistance, low public awareness and engagement

Please state other barriers to innovation in your industry, if any.




Figure 2: Question 2: Please rank the following barriers to innovation in your industry with respect to the usage of IoT devices/systems.

The 3<sup>rd</sup> question of the questionnaire (Figure 3) intended to understand the perspective of the contributors as well as to understand the extent to which IoT devices/systems are actually used by the industry and other sectors.

\* Question 3: What is your company's/institute role within the IoT ecosystem?

- ☐ I do not use IoT devices and am not interested
- ☐ I do not use IoT devices but I am interested in using them in the next 2 years
- ☐ I have a wide spread of IoT devices, properly integrated
- ☐ I use IoT devices but only for marginal activities

Figure 3: Question 3: What is your company's/institute role within the IoT ecosystem?

Question 4 (Figure 4) was along the same direction however, in this case the actual position of the person providing the contribution was requested in order to understand whether the actual position of contributor could have a different perspective. Moreover, this question can provide insides as to the percentages of people occupied at specific positions trying to identify any gaps in the market.

## D1.4 - Continuous Technology Watch and Alignment

\* Question 4: What is your personal role within the IoT ecosystem?

- ☐ Account manager
- ☐ Business analyst
- ☐ Business developer
- ☐ Data engineer
- ☐ Device developer
- ☐ Network engineer
- ☐ Product manager
- ☐ Project manager
- ☐ Quality assurance
- ☐ Sales engineer
- ☐ Sales representative
- ☐ Security specialist
- ☐ Software developer
- ☐ Solutions architect
- ☐ Support engineer

Figure 4: Question 4: What is your personal role within the IoT ecosystem?

The next 2 questions (Question 5 & 6) are directed towards the identification of opportunities in IoT systems 2-5 years forward as well as the most relevant applications for IoT systems in general (Figure 5 & Figure 6).

\* Question 5: What are the key opportunities for IoT systems in the next 2-5 years?



Figure 5: Question 5: What are the key opportunities for IoT systems in the next 2-5 years?

\* Question 6: What do you think that are the most relevant applications?



Figure 6: Question 6: What do you think are the most relevant applications?

Question 7 (Figure 7) focuses on the main implementation challenges towards the adoption &/or growth of IoT systems at the time in their respective industry sectors. Although this question is directly related to the ranking question 2, this open question allows the contributors to provide insides on the existing challenges, that the consortium was not aware of.

\* Question 7: What is preventing the adoption / growth of IoT systems at the moment in your industry segment?



Figure 7: Question 7: What is preventing the adoption/growth of IoT systems at the moment in your industry segment?

Questions 8 & 9 (Figure 8 & Figure 9) are designed to garner insights into the advantages, disadvantages, and potential risks associated with current IoT systems. The answers to these questions will provide significant information about the general benefits and



## D1.4 - Continuous Technology Watch and Alignment

drawbacks of implementing IoT systems today and what the users would like to have in the next 5 years.

\* Question 8: State the 3 main pains, negative situations or risks for your entity with respect to the current IoT systems.



Figure 8: Question 8: State 3 main pains, negative situations or risks for your entity with respect to the current IoT systems.

\* Question 9: State the 3 main gains or positive impact that you would like to see implemented in IoT systems in the next five years.



Figure 9: Question 9: State the 3 main gains or positive impact that you would like to see implemented in IoT systems in the next five years.

Questions 10 & 11 (Figure 10 & Figure 11) are drilling directly to the point, asking the contributors to list the IoT technologies that they are currently using in their respective sector in an attempt to identify which technologies are the most wanted having the highest commercialization interest. Other than just asking for the technologies that are currently used, question 11 is also attempting to pinpoint the intentions to use other IoT technologies in the next 5-10 years. Linking these technologies with the drawbacks identified from the previous questions can highlight the importance of the IoT-NGIN's advancements in the state-of-the-art.

\* Question 10: What IoT technologies are you using now? (e.g., Real-Time Monitoring of your application, System Automation, Remote Control etc.)



Figure 10: Question 10: What IoT technologies are you using right now?

\* Question 11: What are the IoT technologies you plan to use in the next 5/10 years?

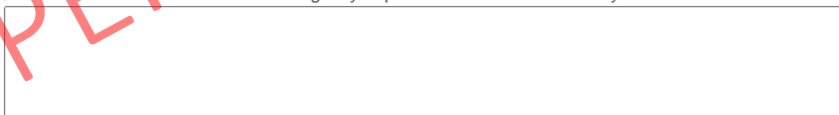


Figure 11: Question 11: What are the IoT technologies you plan to use in the next 5-10 years?

The next question (Figure 12) is a ranking question that focuses entirely on identifying the sectoral and user needs from IoT systems by ranking the profound benefits of installing such systems. Although the results from this question can be analyzed both in terms of each sector, a more horizontal approach can be adopted to identify the needs for IoT systems that can be used in multiple sectors.

## D1.4 - Continuous Technology Watch and Alignment

\* Question 12: Order the following benefits by importance level considering the needs of your industry segment  
Use drag&drop or the up/down buttons to change the order or accept the initial order.

⋮	↑ ↓	Cost savings
⋮	↑ ↓	Enhanced security
⋮	↑ ↓	Improve infrastructure observability
⋮	↑ ↓	Improved customer experience
⋮	↑ ↓	Improved decision making
⋮	↑ ↓	Improved sustainability
⋮	↑ ↓	Increased competitiveness
⋮	↑ ↓	Increased efficiency
⋮	↑ ↓	New business opportunities

Figure 12: Question 12: Order the following benefits by importance considering the needs of your industry segment.

The next question (Figure 13) is using the Key Exploitable Results (KERs) of IoT-NGIN to understand which of these technologies, the industry/market is mostly interested in and maybe even identify in which sectors each one of these KERs would have a higher commercialization interest.

\* Question 13: What kind of IoT related service would you use?  
at most 8 choice(s)

- ☐ 5G Resource Management API
- ☐ AI-based object recognition algorithm using computer vision
- ☐ AR Based Maintenance Services
- ☐ Blockchain based services
- ☐ Crop harvesting assisting framework
- ☐ Decentralised Interledger Bridge
- ☐ Enhanced IoT/5G FeD2D
- ☐ Industrial 5G Core with network slice manager
- ☐ IoT Device Discovery
- ☐ IoT Device Indexing
- ☐ IoT devices access control
- ☐ IoT Vulnerabilities Crawler
- ☐ Malicious Attack Detector
- ☐ ML as a Service platform
- ☐ ML Online Learning framework
- ☐ ML-based precision agriculture modules
- ☐ Model Sharing, Model Translation and Zero Knowledge Verification framework
- ☐ Moving Target Defence (MTD) network of Honeypots
- ☐ Privacy preserving federated ML
- ☐ Privacy-preserving self-sovereign identity solutions
- ☐ Secure Edge Cloud Framework
- ☐ Semantic twin

Figure 13: Question 13: What kind of IoT related service would you use?

The following questions are slightly more specific in terms of technologies in order to obtain more information on what features are really needed from each technological field by the industry. Other than the KERs of IoT-NGIN, question 14 & 15 (Figure 14 & Figure 15) intended to identify and list any technologies that the market/industry is interested in specifically in the area of edge and cloud solutions and digital twins.

## D1.4 - Continuous Technology Watch and Alignment

\* Question 14: What kind of options are you using in terms of edge and cloud solutions and why?



Figure 14: Question 14: What kind of options are you using in terms of edge and cloud solutions and why?

\* Question 15: Is your company using digital twin for asset management?

- ☐ No
- ☐ Yes, but only for minor business processes
- ☐ Yes, for all business processes
- ☐ Yes, only the main business process

Figure 15: Question 15: Is your company using digital twins for asset management?

Questions 16-18 (Figure 16, Figure 17 & Figure 18) are aimed to both obtain information on the future plans of the industry towards the implementation of IoT ecosystem including a time plan as well as the required financial investments.

\* Question 16: Is there any deployment and installation timeline for an standard IoT ecosystem integration on a real industrial environment?

- ☐ The IoT ecosystem has been tested and there is no timeline for installation
- ☐ The IoT ecosystem has been tested and will be installed in the next 2 years
- ☐ The IoT ecosystem has been tested and will be installed in the next 5 years
- ☐ The IoT ecosystem is currently installed
- ☐ The IoT ecosystem will be tested in the next 2 years
- ☐ The IoT ecosystem will be tested in the next 5 years
- ☐ The IoT ecosystem will be tested, but there is no timeline

Figure 16: Question 16: Is there any deployment and installation timeline for a standard IoT ecosystem integration on a real industrial environment?

\* Question 17: Is there any initial cost evaluation of standard IoT ecosystem integration based on technologies defined?

- ☐ Yes
- ☐ No

Figure 17: Question 17: Is there any initial cost evaluation of standard IoT ecosystem integration based on technologies defined?

\* Question 18: Is there any time period estimation for return of investment in deployment of standard IoT ecosystem?

- ☐ No
- ☐ Yes, and the return time is currently excessive
- ☐ Yes, and the return time is currently short

Figure 18: Question 18: Is there any time period estimation for return of investment in deployment of standard IoT ecosystem?

### 3 Survey Results

The results from the questionnaire were obtained directly from the EU Survey website and were analyzed question by question. The analysis with the conclusions drawn from each question is presented in the next section, whilst a list of drawn conclusions is provided in the second subsection of this chapter.

#### 3.1 Survey Analysis

The first question was meant to capture the interest in IoT systems depending on the verticals. As it can be seen from Figure 19, the 3 main verticals are smart energy, Industry 4.0 and smart cities. The result of this question is aligned with IoT-NGIN's claim that the 3 out of 4 verticals investigated within the framework of the project are indeed the most commercially important. Although smart agriculture (4<sup>th</sup> vertical of IoT-NGIN) is not included in the answers, it has been claimed by many researchers that the vertical is still at its infancy with the potential however, to eventually surpass the interest in the energy sector [2] [3].

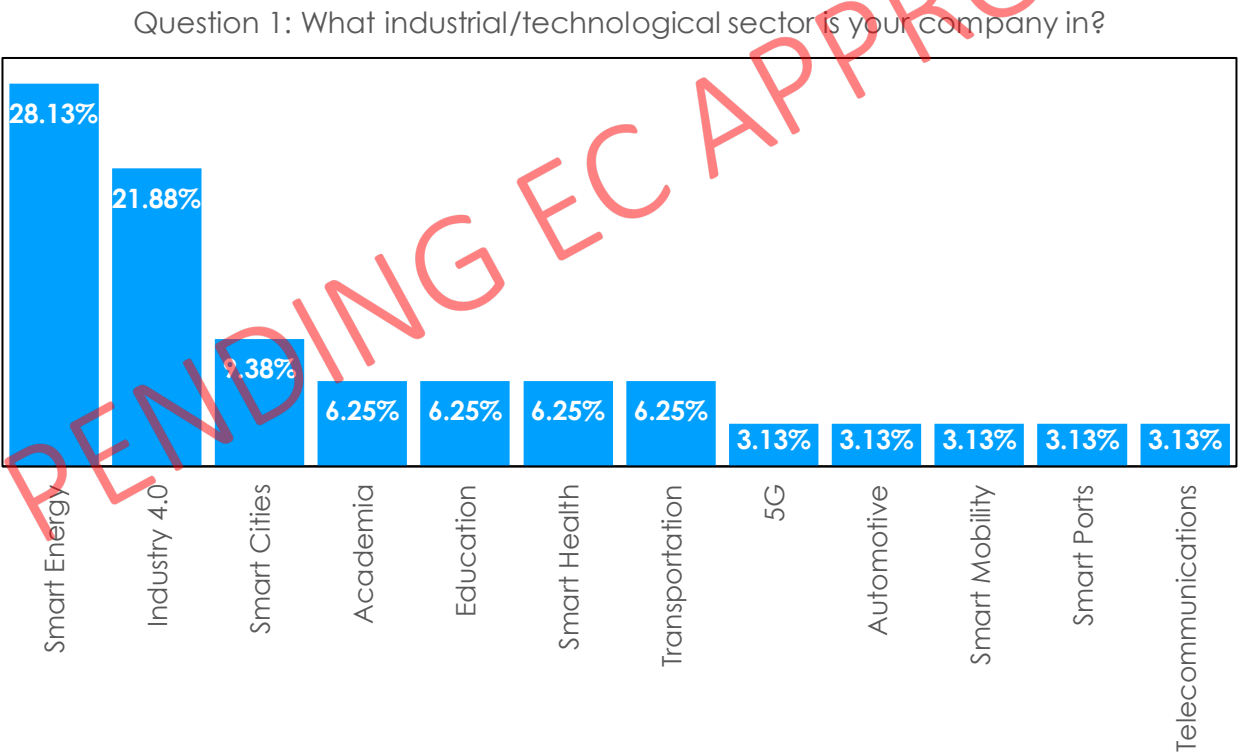


Figure 19: Results from Question 1.

Question 2 aimed to identify the most common challenges faced for the implementation of IoT systems in everyday environments. Figure 20 below shows in a tabulated format the ranking of the challenges. The vertical order of the challenges is the one used in the questionnaire and it is completely random. Under column named "1", the number of times the challenge was placed 1<sup>st</sup> is shown. For example, "Cybersecurity and data privacy" challenge was ranked 1<sup>st</sup> five times out of the 22 contributions received.

## D1.4 - Continuous Technology Watch and Alignment

Based on the obtained results, and looking at them in a more cumulative perspective, "cybersecurity and data privacy" and "Interoperability concerns" are ranked in the top 3 positions for 12 and 11 times out of 22, respectively. This means that they are probably the most common challenges faced. On the other hand, "Network reliability" and "Technology immaturity" are ranked in the last 3 positions for 12 and 11 times, respectively. Once more, this probably means that they are the challenges that are faced the least.

	Ranking											
	1	2	3	4	5	6	7	8	9	10	11	12
Cybersecurity and data privacy	5	2	5	3	1	3	1	0	1	1	0	0
High CAPEX	3	2	2	1	1	2	2	3	0	4	2	0
High OPEX	2	2	0	2	2	2	2	2	3	0	2	3
Interoperability concerns	5	2	6	2	4	0	1	1	1	0	0	0
Lack of infrastructure	0	4	1	3	2	2	3	4	0	0	3	0
Lack of necessary technical skills & knowledge	2	4	1	2	0	2	1	3	2	2	2	1
Lack of open standards	1	4	2	1	1	2	6	0	2	3	0	0
Market uncertainty	1	0	1	4	2	2	0	2	2	2	5	1
Network reliability	0	0	1	1	3	0	2	0	3	5	2	5
Scalability	0	2	1	3	1	2	2	1	2	2	3	3
Technology immaturity	1	0	0	0	3	1	1	3	2	2	3	6
User's resistance, low public awareness and engagement	2	0	2	0	2	4	1	3	4	1	0	3

Figure 20: Results from Question 2: Please rank the following barriers to innovation in your industry with respect to the usage of IoT devices/systems.

The 3<sup>rd</sup> and 4<sup>th</sup> questions (Figure 21 & Figure 22) were meant to understand the role of the companies/institutions in the IoT ecosystem and more specifically, the position of the person that provided their perspective. The vast majority of the companies/institutions, 88%, are either extreme users of IoT systems and they have them implemented and integrated in their everyday operations or they are using them for marginal purposes, when the application and probably the monitoring of certain things is critical.

From the results of question 4, it is obvious that the given perspective is provided in its majority by project managers, solution architects, business analysts and business developers. This is interesting because it means that the perspective is provided at a very

## D1.4 - Continuous Technology Watch and Alignment

high-level, looking at the bigger picture whilst it is expected that most technical details and low-level challenges are not recorded. Furthermore, due to the high-level perspective of most of the contributors, a lot of weight shows up on cost, cybersecurity and data privacy whilst, engineers or developers for example, would value other parameters higher.

Question 3: What is your company's/institute role within the IoT ecosystem?

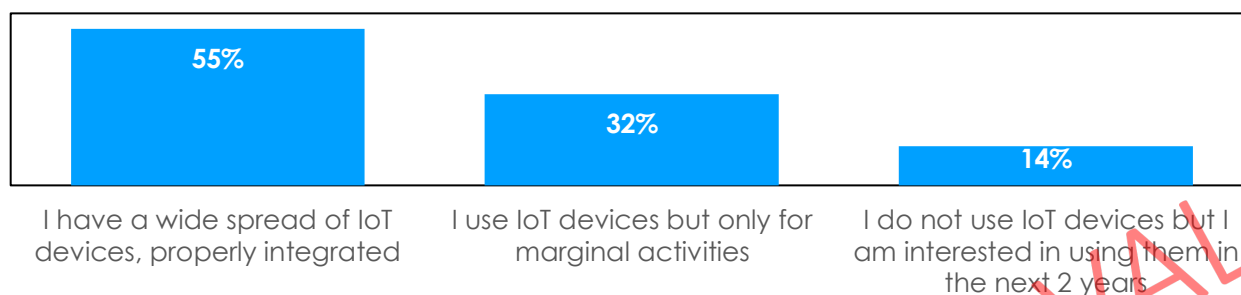


Figure 21: Results from Question 3.

Question 4: What is your personal role within the IoT ecosystem?

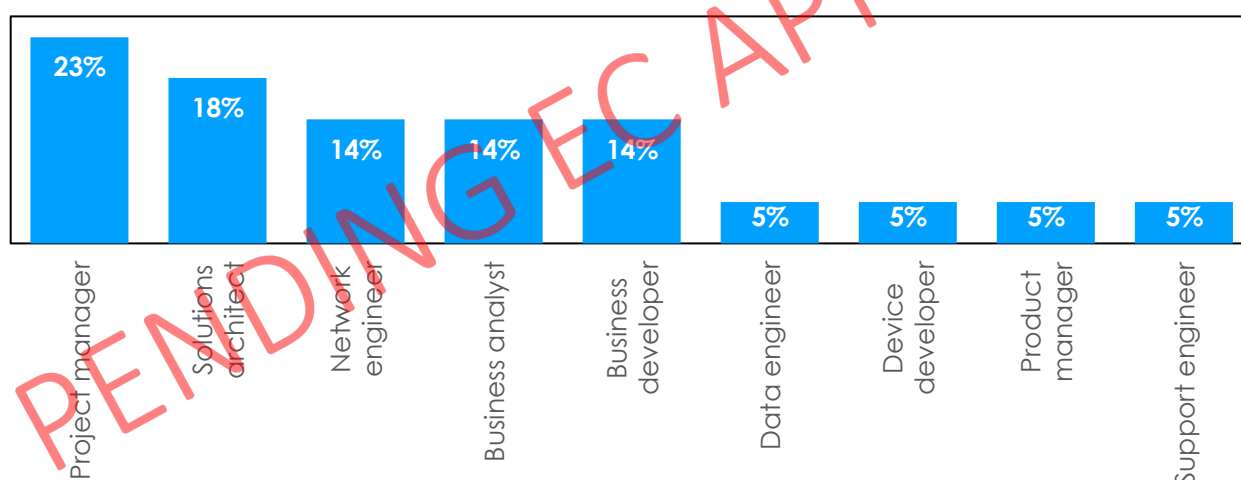


Figure 22: Results from Question 4.

The next question was meant to capture the possible IoT opportunities for the next 2-5 years. Based on the results shown in Figure 23, there is a huge variety of opportunities identified. Nevertheless, the opportunities that showed up mostly were decision support, real-time monitoring and energy management. Once again, these results are in alignment with the proposed opportunities by the IoT-NGIN consortium and are the ones that the exploitation activities of the project focus on.

Other than the 3 main opportunities, event prediction and digital twins domains are also showing up significantly in the results showing a rising interest in that direction.

D1.4 - Continuous Technology Watch and Alignment

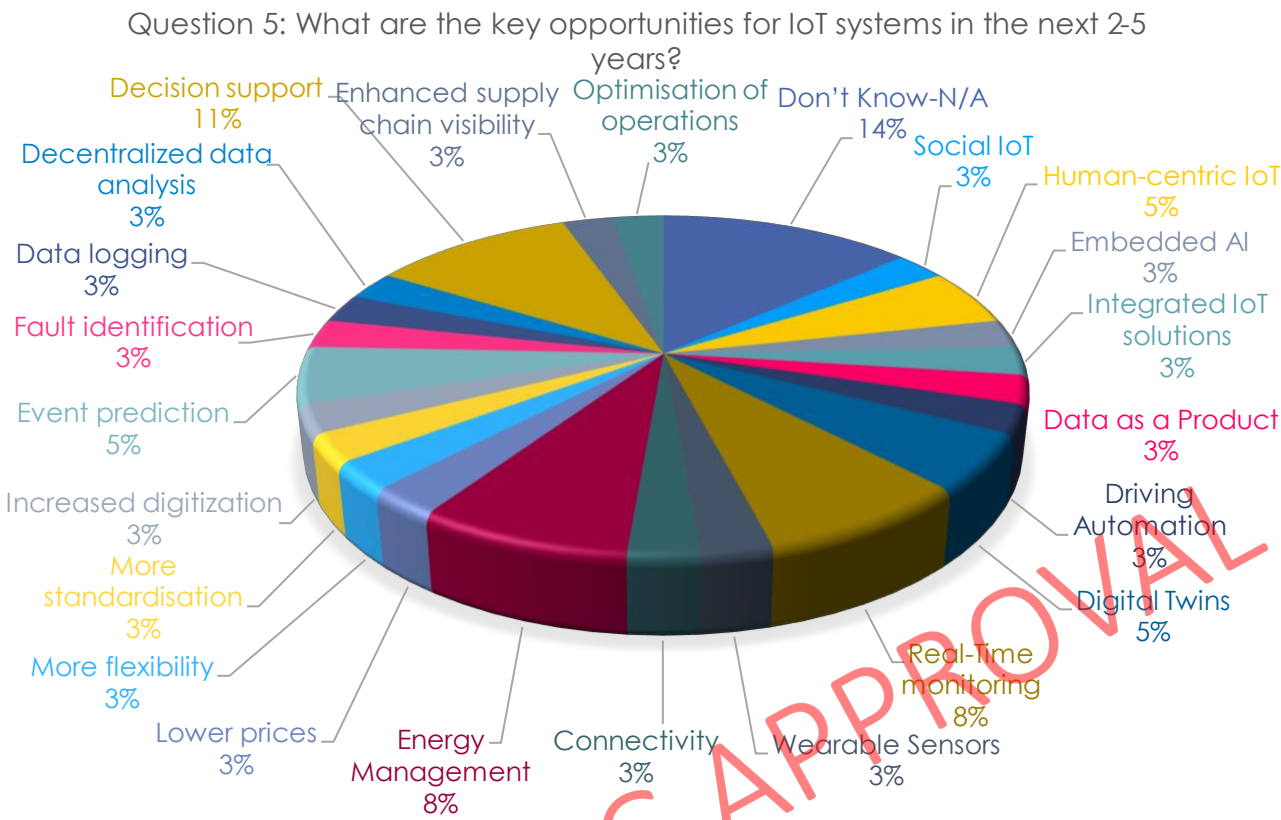


Figure 23: Results from Question 5.

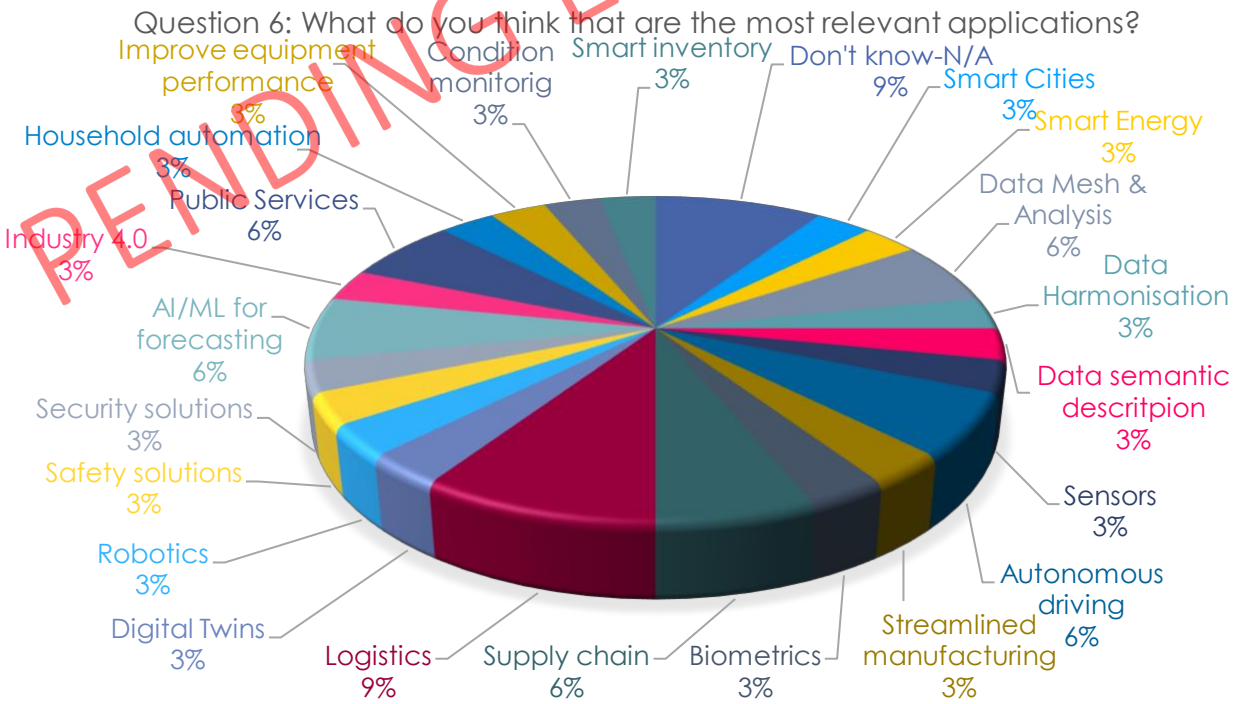


Figure 24: Results from Question 6.



## D1.4 - Continuous Technology Watch and Alignment

In conjunction with question 5, question 6 tries to place the aforementioned technological opportunities in the application domain. Based on the obtained results, the most common domains are logistics, public services, AI/ML for forecasting, supply chain, autonomous driving and data mesh & analysis. The applications/domains identified are again in alignment with the use cases and Living Labs within the IoT-NGIN's framework.

Although several opportunities and applications were identified in the previous questions, question 7 aims to understand what IoT systems are as widely used as they could be. Based on the results presented in Figure 25 below, the most important and most common stumbling block is the lack of investments on equipment needed as well as the fact that there are not enough standards for such IoT systems. These results back up the claim of the IoT-NGIN project that enhancement of the underlying IoT technologies is required so that the cost of the equipment can be significantly decreased. Furthermore, IoT-NGIN has indeed contributed to the development of new standards hence, addressing the most common stumbling blocks towards the adoption of IoT systems and technologies.

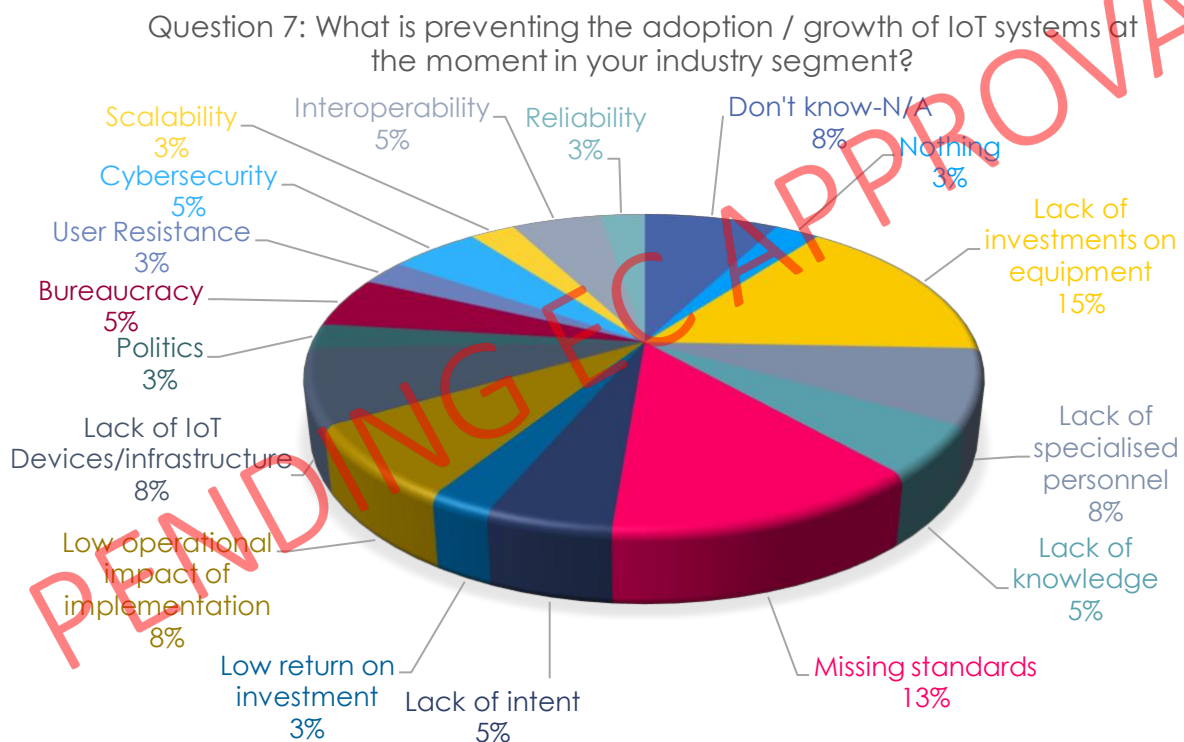


Figure 25: Results from Question 7.

Questions 8 & 9 aims to capture the pains and gains from the implementation of IoT systems in the respective domain of the company that is filling in the questionnaire. Based on the results shown in Figure 26 & Figure 27 below, the most common pains are security & privacy, lack of standards and cost. On the other hand, the most common gains recorded are the semi-automation of decision-making/support and the improved efficiency of operations.



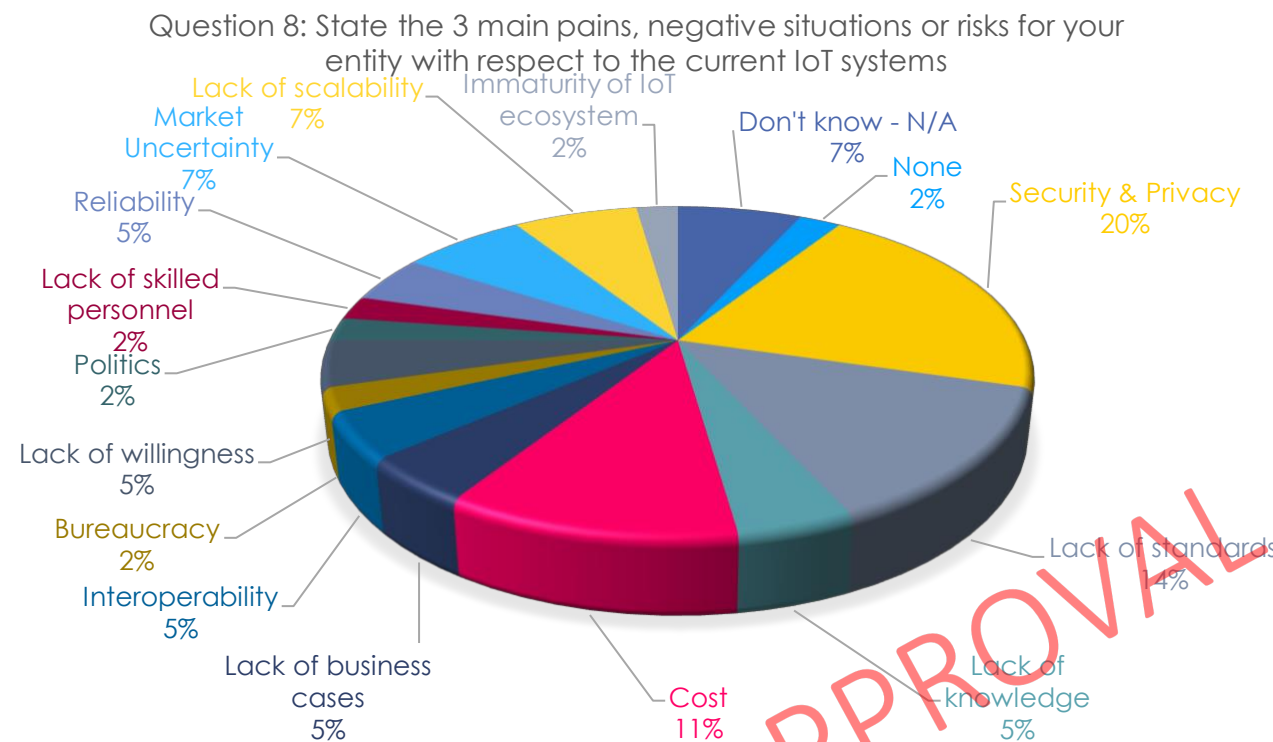


Figure 26: Results from Question 8.

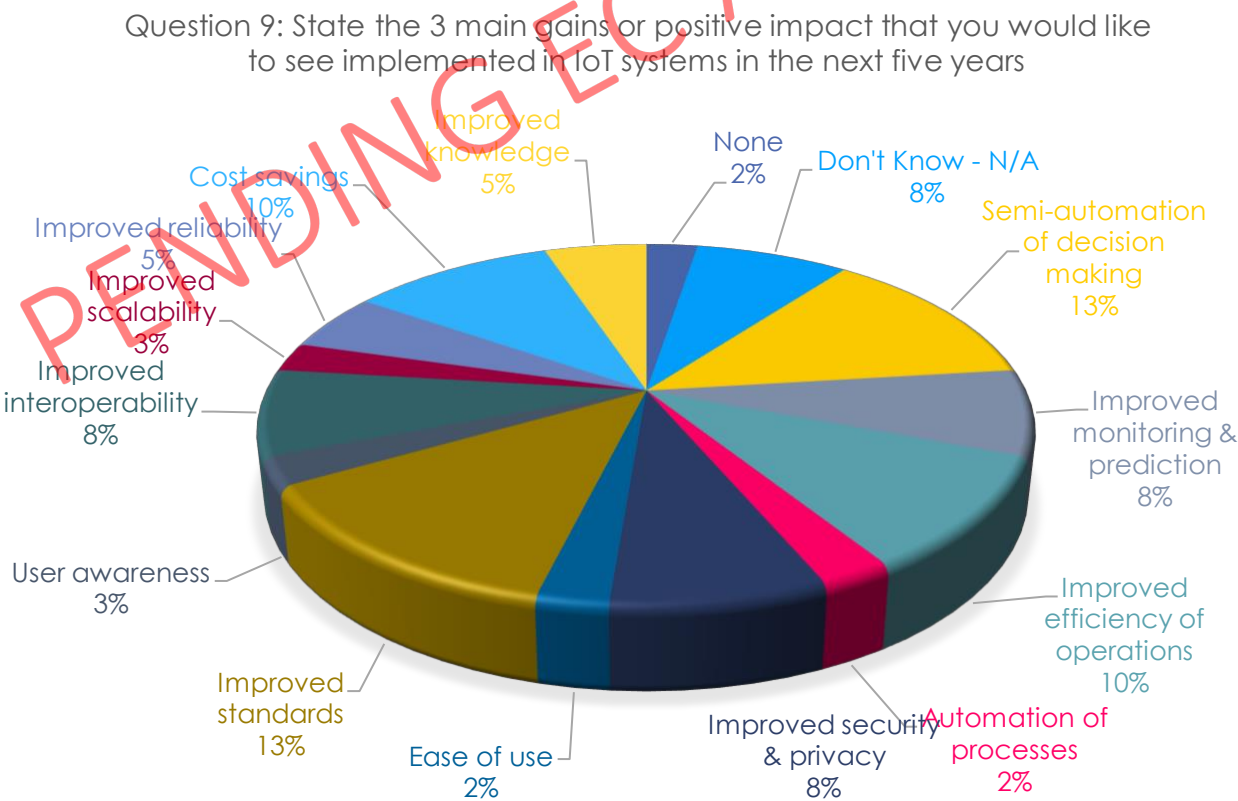


Figure 27: Results from Question 9.

## D1.4 - Continuous Technology Watch and Alignment

Question 10 is trying to capture the actual IoT technologies that are currently being used. Based on the results in Figure 28, three technologies make the vast majority of the answers. Monitoring technologies, remote control and system automation are actually the ones used at the moment showing a higher maturity level of these technologies compared to artificial intelligence, for example.

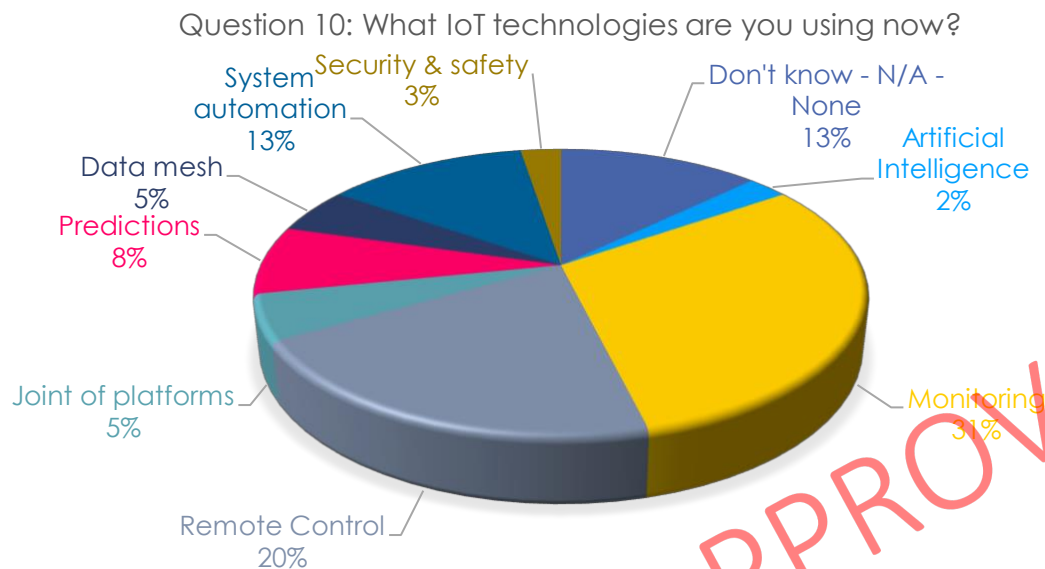


Figure 28: Results from Question 10.

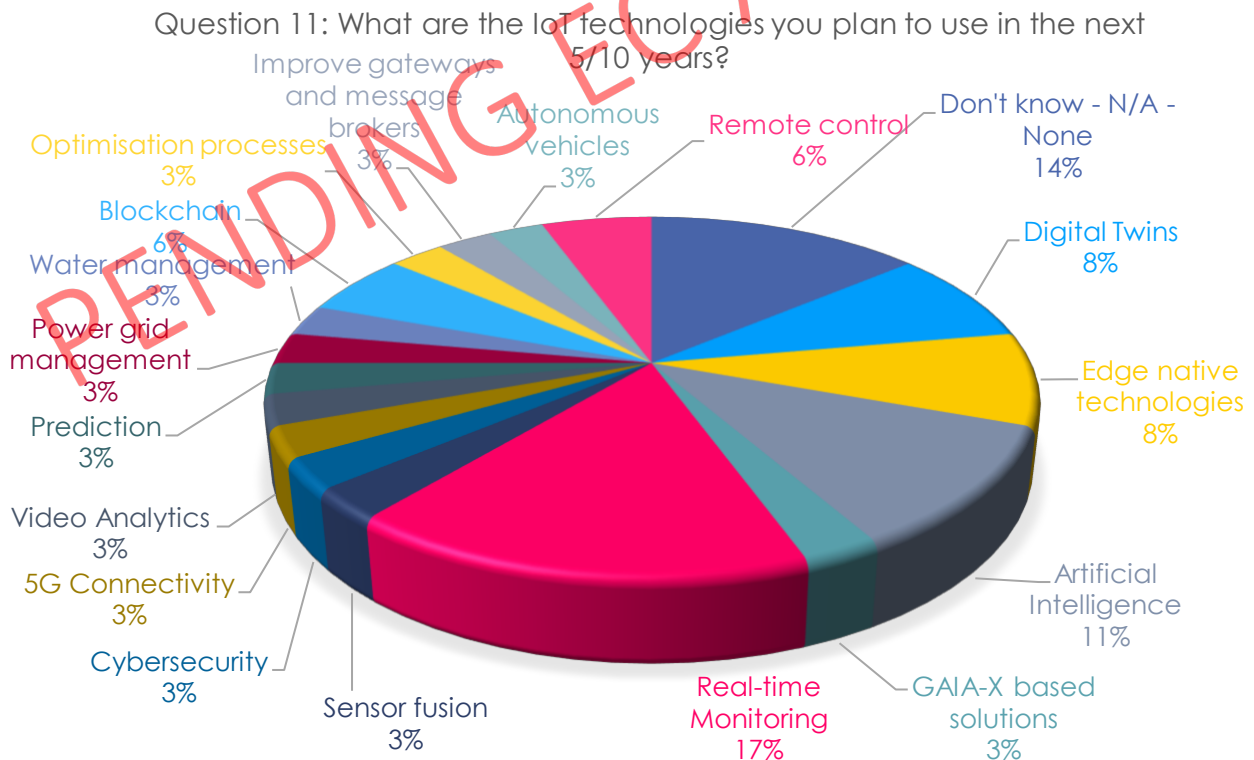


Figure 29: Results from Question 11.

## D1.4 - Continuous Technology Watch and Alignment

Since most of the information about the current status of IoT systems in the market has been obtained, at least at an indicative level, question 11 aimed to capture the future predictions on the possible IoT technologies to be implemented in the next 5-10 years. Figure 29 shows the obtained results, which highlight the rising trends in the real-time monitoring, artificial intelligence, digital twins and edge native technologies. The technological development work within IoT-NGIN has mainly focused on these technologies putting the project's work at the forefront of the next generation IoT systems.

Question 12 was looking to identify the driving force for the market to implement IoT systems but also to understand the importance of each reason. Figure 30 below shows how the benefits were ranked based on importance in a similar way as question 2. It is clear that the most important benefit is cost savings since it has been ranked in the top 3 positions for 13 times together with the improved infrastructure observability and improved decision-making that were ranked in the top 3 places for 11 and 10 times, respectively. On the other side of the scale, the least important benefit seems to be the increased competitiveness and the new business opportunities, which were ranked in the last 3 positions for 14 and 12 times, respectively.

	Ranking								
	1	2	3	4	5	6	7	8	9
Cost savings	7	5	1	1	3	1	1	1	2
Enhanced security	2	6	1	2	3	3	0	4	1
Improve infrastructure observability	2	2	7	1	3	1	2	2	2
Improved customer experience	4	1	1	7	3	2	2	1	1
Improved decision making	1	4	5	0	4	3	3	1	1
Improved sustainability	2	0	2	1	2	7	3	3	2
Increased competitiveness	0	1	3	1	2	1	8	4	2
Increased efficiency	1	1	2	6	2	2	2	5	1
New business opportunities	3	2	0	3	0	2	1	1	10

Figure 30: Results from Question 12: Order the following benefits by importance considering the needs of your industry segment.

Question 13 is a more technical question, asking which IoT services would the contributor use. Based on the obtained results shown in Figure 31, there is a significant spread of services that are attractive to the contributors since the answers are not focusing on specific services. Nevertheless, the most common answers are the use of the AI-based, object recognition algorithm using computer vision, the secure edge cloud framework and the ML as a Service Platform. Although the least interesting technologies are the ones related to smart agriculture, those answers do not represent the smart agriculture market because none of the contributors in this survey is actually coming from that domain.

Question 13: What kind of IoT related service would you use?

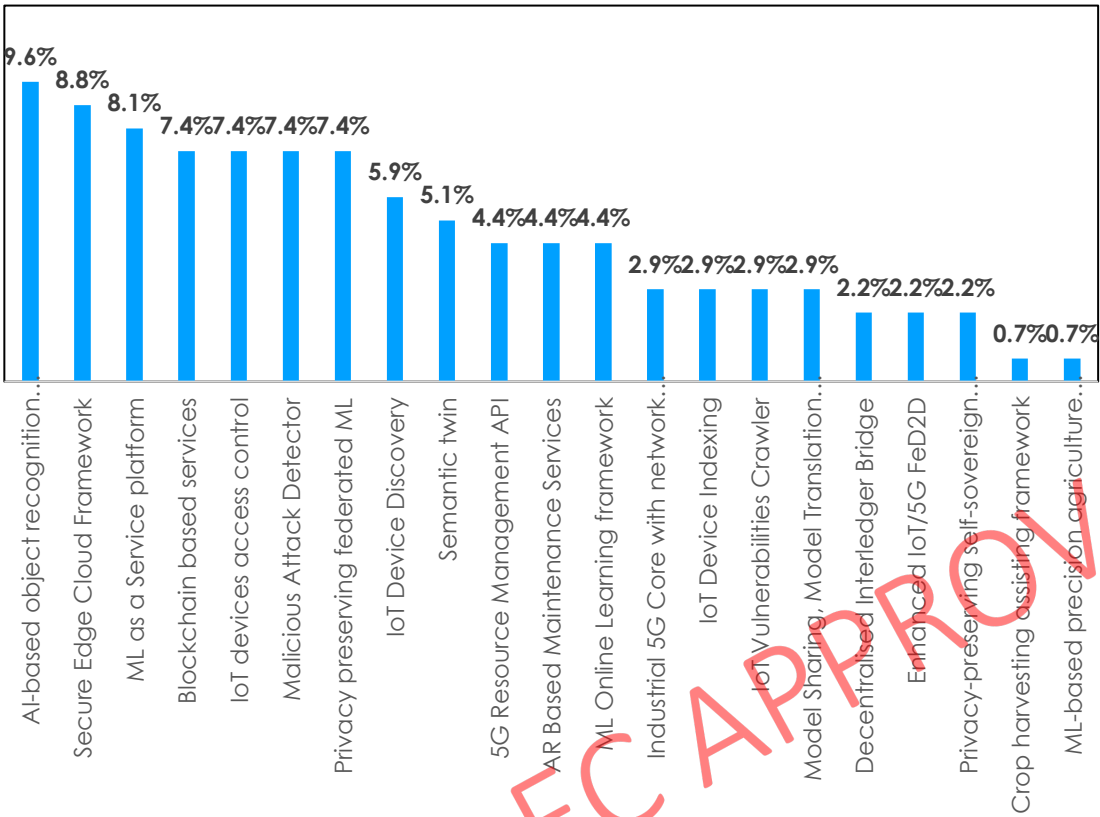


Figure 31: Results from Question 13.

Question 14: What kind of options are you using in terms of edge and cloud solutions and why?

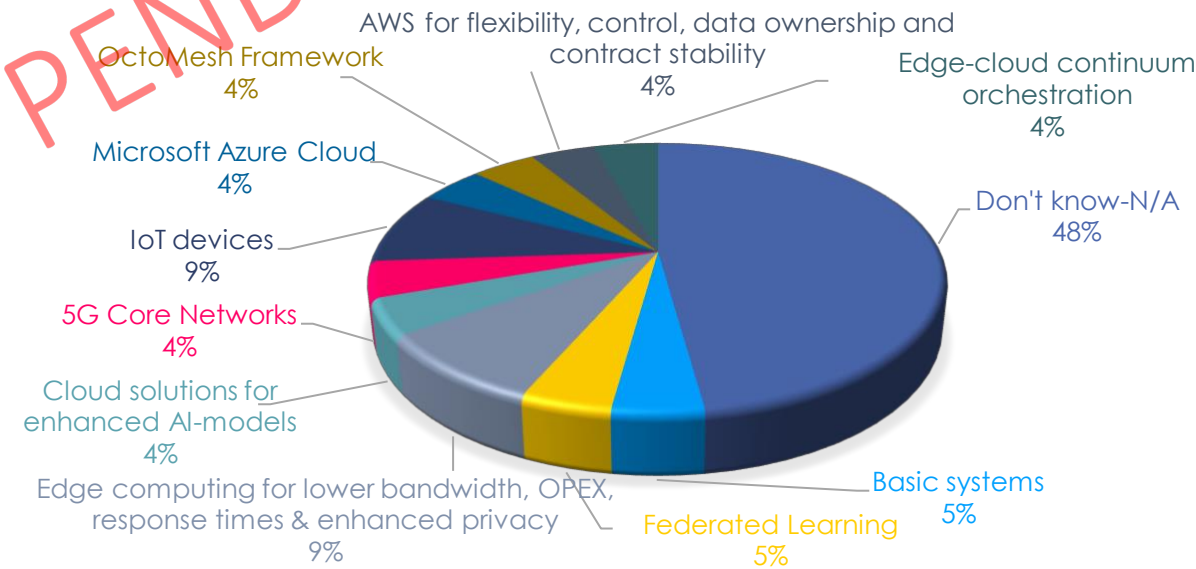


Figure 32: Results from Question 14.

D1.4 - Continuous Technology Watch and Alignment

Question 14 is trying to see what the preferred options are for edge and cloud solutions. From the results shown in Figure 32, the vast majority is still unaware of the available solutions in this field and those who are aware are focusing mostly on IoT Devices and edge computing for lower bandwidth, OPEX, response times & enhance privacy.

Question 15 was specifically looking into the use of digital twins for asset management. The results (Figure 33) suggest that the implementation of digital twins for asset management at the current stage is only used for minor processes or not at all. Only a very small minority of users have implemented it for all business processes.

Question 15: Is your company using digital twin for asset management?

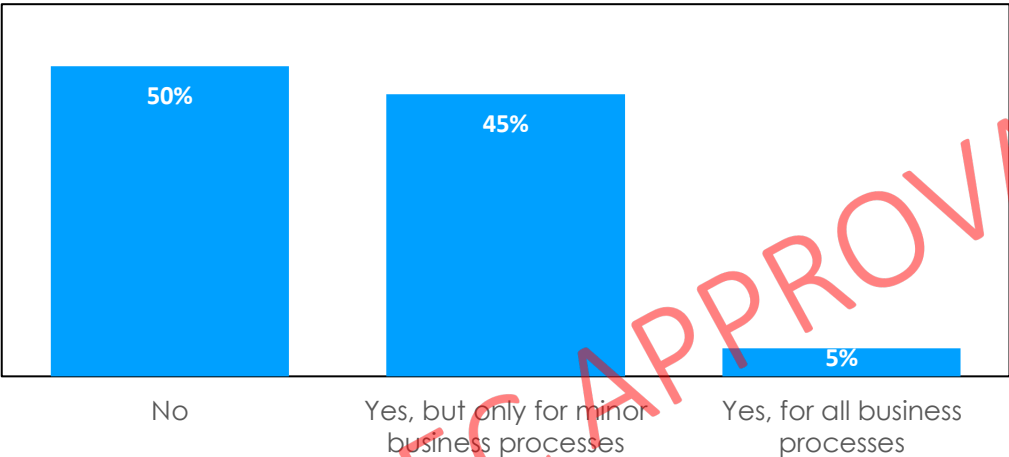


Figure 33: Results from Question 15.

The last 3 questions are targeting the future trends in the deployment of IoT systems in an industrial environment whilst understanding is a budgeting and a timeline is identified for that installation.

Question 16: Is there any deployment and installation timeline for an standard IoT ecosystem integration on a real industrial environment?

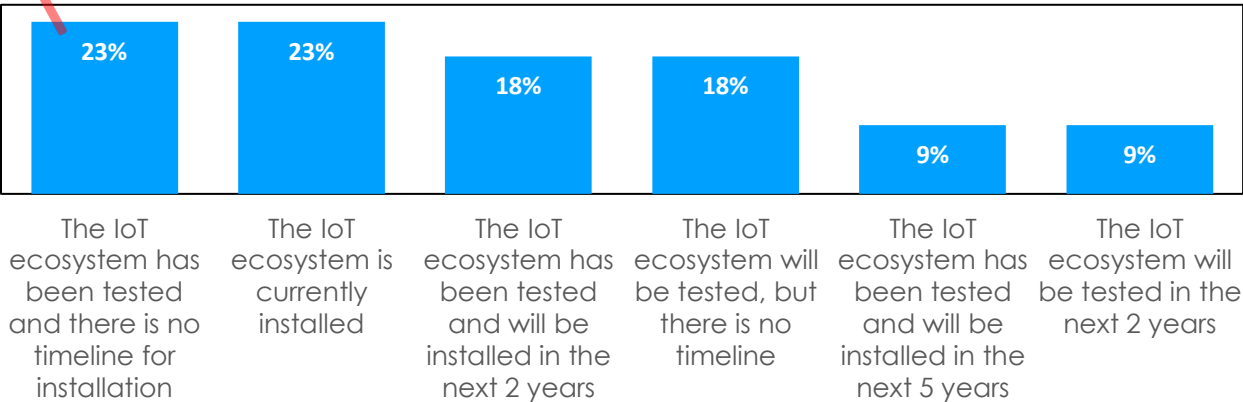


Figure 34: Results from Question 16.

Question 17: Is there any initial cost evaluation of standard IoT ecosystem integration based on technologies defined?

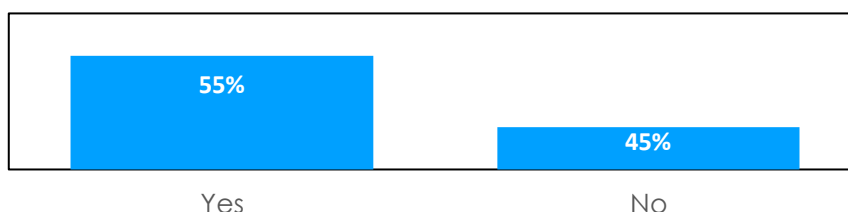


Figure 35: Results from Question 17.

Question 18: Is there any time period estimation for return of investment in deployment of standard IoT ecosystem?

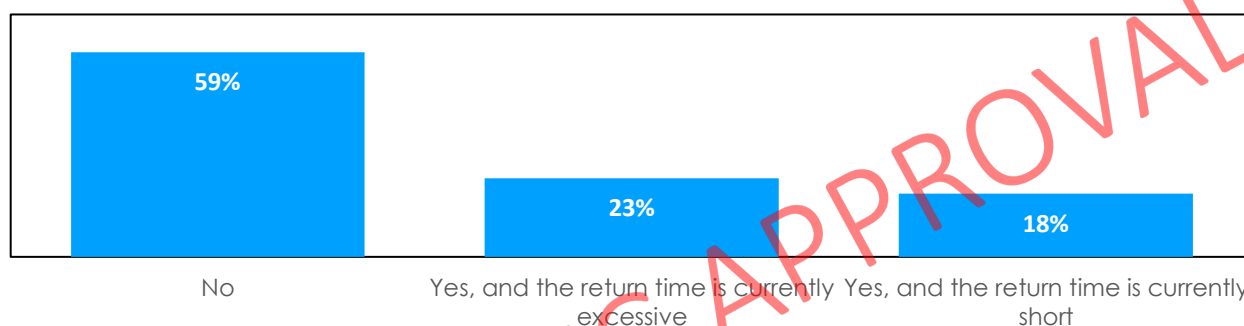


Figure 36: Results from Question 18.

Based on the obtained results shown in Figure 34, Figure 35 & Figure 36, the users have either tested and installed the proposed IoT system or they are not planning to invest to implement new IoT systems with their current status.

## 3.2 Survey Conclusions Summary

A comprehensive but summarized version of the conclusions drawn is provided below:

1. The three main verticals of interest for IoT systems are smart energy, Industry 4.0, and smart cities, aligning with IoT-NGIN's focus on commercially important sectors.
2. The most common challenges in implementing IoT systems are cybersecurity and data privacy, as well as interoperability concerns. IoT-NGIN's efforts in addressing these challenges are crucial for wider adoption.
3. Contributors' perspectives mainly come from high-level roles such as project managers and solution architects, potentially missing technical details and low-level challenges.
4. Decision support, real-time monitoring, and energy management are key IoT opportunities for the next 2-5 years, alongside rising interest in event prediction and digital twins.
5. Applications for IoT systems are prevalent in logistics, public services, AI/ML for forecasting, supply chain, autonomous driving, and data mesh & analysis, aligned with IoT-NGIN's use cases and Living Labs.

## D1.4 - Continuous Technology Watch and Alignment

6. Lack of investments in equipment and insufficient standards are major stumbling blocks for wider IoT adoption, reinforcing the importance of IoT-NGIN's focus on enhancing underlying IoT technologies and contributing to new standards.
7. The most common pains from IoT implementation are security & privacy concerns, lack of standards, and cost issues, while the most common gains are semi-automation of decision-making/support and improved operational efficiency.
8. Monitoring technologies, remote control, and system automation are the most widely used IoT technologies currently, showing higher maturity compared to other technologies.
9. Future trends point towards increasing interest in real-time monitoring, artificial intelligence, digital twins, and edge native technologies, areas where IoT-NGIN has been actively working.
10. The primary driving force for implementing IoT systems is cost savings, followed by improved infrastructure observability and improved decision-making, while increased competitiveness and new business opportunities are of lower importance.
11. AI-based object recognition, secure edge cloud framework, and ML as a Service Platform are among the most attractive IoT services for contributors.
12. Contributors are generally unaware of available edge and cloud solutions, but those who are aware focus on IoT devices and edge computing for specific benefits.
13. Digital twins for asset management are still at an early stage of implementation, with only a small minority using them for all business processes.
14. Users have either tested and installed proposed IoT systems or are not planning to invest in new IoT systems in industrial environments with their current status.

PENDING EC APPROVAL



## 4 Continuous Technology Watch

### 4.1 Technologies Identified for the 4 Verticals

D1.3 provided a snapshot of a technology watch of available and relevant technologies for the 4 verticals of the project and beyond. These technologies are adopted and somehow extended by the project in the development of the project technical components and their adoption in the use cases of the Living Labs. This section summarizes the main technologies collected in D1.3 [2] technology watch for the convenience of the reader. This collection is also complemented with those technologies mentioned in the survey of section 3.

These technologies are listed in Table 1 below:

Table 1: List of identified technologies.

No.	Technologies	Subcategories
1	Devices	<ul style="list-style-type: none"> <li>Cameras equipped with AI               <ul style="list-style-type: none"> <li>Video analytics</li> </ul> </li> <li>Traffic sensors</li> <li>IoT parking sensors</li> <li>High density sensor networks</li> <li>Satellite imaging</li> <li>On-the-go sensors</li> <li>Remote control               <ul style="list-style-type: none"> <li>Drones (with cameras)</li> <li>Robotic arms and vehicles</li> </ul> </li> <li>Autonomous guided vehicles               <ul style="list-style-type: none"> <li>Autonomous robots with cameras</li> </ul> </li> <li>Phone cameras</li> <li>Sensor fusion</li> </ul>
2	Models	<ul style="list-style-type: none"> <li>Simulation models</li> <li>Statistical models</li> <li>ML models</li> <li>Hybrid models</li> </ul>
3	Artificial Intelligence	<ul style="list-style-type: none"> <li>ML operations (MLOps)</li> <li>AI-based computer vision</li> <li>Meta-learning               <ul style="list-style-type: none"> <li>Zero-shot learning</li> <li>Few-Shot learning</li> <li>One-Shot learning</li> <li>AI-based Optimization</li> </ul> </li> </ul>
4	Augmented Reality	
5	Visualization technologies	



6	Computer Assisted Design (CAD)	
7	Communications technology	<ul style="list-style-type: none"> <li>• 5G connectivity</li> <li>• Ultra-broadband</li> </ul>
8	Gateways and message brokers	
9	Digital Twins	
10	Real-time monitoring	
11	Cybersecurity	Blockchain

## 4.2 Opportunities Identified for the 4 Verticals

### 4.2.1 Smart Cities

The Internet of Things sector offers numerous perspectives and opportunities for the development of smart cities, for example in applications such as traffic flow forecasting, parking and crowd management and interaction with social media.

Implementing IoT in these areas can improve traffic efficiency and optimize parking space utilization. Placing smart sensors for traffic monitoring can enable the collection of detailed road traffic data in real time. These sensors can be installed on roads, intersections or even on vehicles themselves, allowing accurate detection of traffic flow and more precise forecasting. Data collected by IoT sensors can be processed using advanced data analysis algorithms, such as machine learning and artificial intelligence. This allows you to identify patterns and trends in traffic and generate accurate forecasts about future traffic flow. Traffic forecast information can be used to optimize routes, reduce travel times and improve road safety.

Applied to the smart parking industry, IoT can be used to create intelligent parking management systems. Parking sensors can detect parking occupancy and transmit the data in real time to a central system. Information about available parking spaces can be viewed on mobile apps or information panels, allowing drivers to quickly locate vacant spaces. This reduces traffic congestion caused by finding parking and improves the overall parking experience.

Both of the above applications can be integrated for navigation and intelligent routing: drivers can receive directions avoiding congested areas or alternative suggestions to reach their destination more efficiently.

Finally, traffic and parking management through specific analytics allows local authorities to efficiently plan changes to urban mobility, allowing targeted interventions, such as the synchronization of traffic lights or the creation of preferential lanes for public transport.

A further application concerns the management of queues and crowds in smart cities. Implementing IoT solutions in this area can improve the efficiency of operations, optimize the user experience, and ensure public safety.

Placing smart sensors in public places, such as stations, government offices, hospitals and entertainment venues allow you to obtain information to be included in tools on how to optimize the flow of people and reduce waiting time. It is also possible to integrate this information to improve the quality of service for users, for example through apps that update users on waiting times and plan activities. From a security point of view, this information avoids and prevents overcrowding and allows high-risk areas to be identified and allows authorities to plan and take more effective preventive measures.

Social networks can play different roles within smart cities, helping to improve communication, citizen participation and information sharing.

Social networks offer an immediate and two-way communication channel between citizens and local authorities. Social media platforms allow people to stay up to date on emergency alerts, safety alerts, local news, and events. At the same time, people can provide feedback, report problems or share ideas with authorities through social networks. This facilitates the involvement of citizens in the life of the city and promotes greater participation in its management. Local authorities can monitor citizens' conversations and feedback on social media to gain insight into their needs, preferences and concerns. This information can be used to make more informed decisions in urban policy planning and management.

Authorities can use social media to advertise public transport services, recycling programs, cultural events or environmental awareness campaigns. This helps to improve the visibility of initiatives and increase citizen participation.

In summary, from the point of view of the smart grid, a radical change is expected thanks to the availability of numerous data from distributed sensors or social media, in order to improve the quality of life of citizens.

### 4.2.2 Smart Agriculture

The agriculture sector can benefit significantly from the introduction of IoT devices and the application of analytics, for example in the field of disease prediction in agricultural crops, smart irrigation, precision aerial spraying and sensor-assisted harvesting of agricultural crops. Implementing IoT in these areas can improve crop management, optimize resource use, and increase overall agricultural productivity.

Placing smart sensors for crop monitoring can enable analysis of environmental conditions (soil moisture, temperature, air humidity, sunlight level and air quality) in real time. Using data analysis algorithms, such as machine learning algorithms and artificial intelligence, sensors can detect early signs of disease or stress in plants, allowing farmers to take early action to prevent or mitigate their impact.

IoT can be used to create smart irrigation systems that tailor irrigation to actual crop needs. IoT sensors can detect soil moisture and other parameters, transmitting the data to a central system. This system can then process the data and provide precise guidance on irrigation, optimizing water consumption and preventing waste. Smart irrigation helps keep crops in optimal condition and improve water efficiency. A specific application is

that of precision aerial spraying, through thrusters or other IoT devices. Precision aerial spraying allows treatments to be applied only where and when needed, reducing the consumption of chemicals and minimizing the impact on the environment.

Through mobile apps or web dashboards, farmers can view real-time data, make data-driven decisions, and check the status of the agricultural field. This increases the flexibility and efficiency of agricultural operations.

A further application is those of sensor-assisted harvesting of agricultural crops. Implementing IoT in these areas can improve harvesting efficiency, optimize resource use, and increase overall agricultural productivity.

The use of smart IoT sensors can enable monitoring of the condition of agricultural crops during the harvesting process. Sensors can detect parameters such as ripening level, fruit quality or the presence of disease or damage. This data can be collected in real time and transmitted to a central system for the analysis and management of collection activities.

In addition, IoT can help optimize harvest times by monitoring crop conditions. Sensors can detect the degree of ripeness or other parameters that indicate the ideal time for harvesting. This allows farmers to plan and schedule harvesting activities optimally, avoiding premature or late harvesting.

Sensors can detect the weight or amount of product harvested, allowing an accurate estimate of the overall yield. This information can be used to evaluate the efficiency of the collection process, optimize future operations, and make informed resource management decisions.

From the point of view of safety and industry regulations, IoT can allow the tracking and traceability of agricultural products during the harvesting process. Using technologies such as QR codes or RFID tags, specific information can be associated with each product collected. This allows you to keep track of origins, cultivation practices, storage conditions and other relevant information. Traceability of agricultural products helps ensure quality, safety and regulatory compliance throughout the supply chain.

In summary, the prospects in the IoT sector for the agricultural sector offer important advantages. The use of smart sensors, real-time monitoring, automation and traceability allow for more efficient and precise management of cultivation and harvesting, improving the efficiency and quality of the overall process.

### 4.2.3 Smart Industry

The Internet of Things sector offers numerous opportunities in the industrial sector, for applications such as increasing human safety in factories or integrating with augmented reality capabilities to increase production efficiency.

For safety management, implementing IoT in these areas can enable better risk management, monitoring of working conditions and timely intervention in emergency situations.

The use of smart IoT sensors can enable monitoring of working conditions within factories. These sensors can detect parameters such as temperature, humidity, pressure, toxic gas levels, noise and vibration. The data collected by the sensors can be transmitted in real

time to a central system, allowing constant supervision of working conditions. This helps identify potential security risks and take appropriate preventive measures.

IoT data analytics can provide valuable insights for risk management in industrial factories. The data collected by the sensors can be processed using advanced data analysis algorithms to identify trends, patterns and anomalies. This allows you to identify potential security risks and take specific preventive measures to mitigate those risks.

IoT can enable real-time incident monitoring and immediate response to emergencies. By connecting IoT devices and sensors to security networks, dangerous situations such as fires, gas leaks or equipment malfunctions can be detected early. The collected data can trigger automatic alerts and initiate predefined response procedures, such as fire alarm or evacuation.

The combination of the Internet of Things and augmented reality offers numerous perspectives and opportunities in the industrial component assembly industry. The implementation of these technologies can improve the efficiency, accuracy and safety of assembly processes, allowing better support to operators. IoT can be used to monitor and manage assets used in the assembly of industrial components. IoT sensors can be integrated into machinery, equipment and components themselves, enabling real-time data on asset performance, status, and utilization. This information can be used for preventive maintenance, resource optimization, and service planning, ensuring efficient and continuous assembly operations. Augmented reality can provide visual and interactive support to operators during the assembly process. Through the use of glasses or AR devices, operators can view assembly instructions superimposed on the real world. Instructions can include animations, images, or text that guide the operator step-by-step through the correct assembly operations. This reduces errors, improves accuracy and speeds up the assembly process. IoT and augmented reality can be used for real-time quality control during the assembly process. IoT sensors can collect data on the quality parameters of assembled components, such as dimensional measurements, structural integrity, or functionality. This data can be displayed in real time through AR devices, allowing operators to perform a visual check and verify the conformity of components. In case of non-compliance, immediate corrective instructions are given, improving the quality of the final product.

These applications can also be adopted for maintenance and remote assistance of assembly plants. IoT sensors can collect data on the performance and status of machinery, allowing potential problems or failures to be identified early. Using AR devices, operators can receive maintenance or service instructions directly in the field, reducing downtime and improving the efficiency of assembly operations.

In summary, the prospects in the field of IoT and augmented reality for human safety in industrial factories and for the assembly of industrial components offer important advantages in terms of efficiency, precision and safety. Using intelligent sensors, real-time monitoring, interactive visual guidance and remote assistance improves risk management, emergency response and optimizes assembly operations, improves product quality and provides advanced support to operators.

## 4.2.4 Smart Energy/Grid

The electricity distribution sector is experiencing a transition period in order to achieve the targets set for the fight against climate change and the reduction of climate-altering emissions.

The Internet of Things sector offers many prospects and opportunities in the field of smart grids. The implementation of IoT in smart grids can improve the efficiency, reliability and sustainability of the overall energy system and foster integration with electric mobility.

IoT can enable real-time monitoring of energy consumption and intelligent energy management in smart grids. Smart meters collect data on users' energy consumption and transmit it to a central system. This data can be used to optimize energy distribution, manage energy demand more efficiently and prevent any overload problems or power outages, facilitate the integration of non-programmable renewable energy sources (solar and wind).

IoT can enable advanced automation and control of electrical distribution networks. IoT devices can be used to intelligently monitor and control grid components, such as transformers, switches or energy storage devices. This allows more efficient management of energy flow, automatic recovery in case of interruptions and better optimization of network operations.

Using predictive maintenance tools, based on distributed sensors, it is possible to detect in advance the emergence of any failures or malfunctions of the network components. Using IoT sensors, data can be collected on the health and performance of components, applying data analysis algorithms to identify signs of deterioration or anomalies. This enables timely and targeted maintenance, reducing costs and optimizing resource utilization.

A further application is that of IoT devices integrated into the electric mobility sector, favoring efficient charging processes, optimizing the use of renewable energy resources and offering a better experience to users.

Smart charging infrastructure for electric vehicles can be created. IoT sensors can be integrated into charging stations to monitor charging conditions, outlet availability and wait times. This information can be passed on to charging station operators and users, allowing for better planning of charging operations and reducing waiting times.

By inserting On-Board-Devices into vehicles, the status of electric vehicle batteries and the optimization of charging are monitored. IoT sensors can collect data on the state of charge, temperature, and other key information of batteries. Using data analysis algorithms, charging can be optimized based on battery needs, extending battery life, reducing charging time, and improving overall energy efficiency.

IoT sensors can be installed on vehicles in a corporate or car-sharing fleet to monitor their usage, location, performance and conditions. This information can be used to optimize fleet operations, such as route planning, preventive maintenance and energy consumption monitoring. This enables more efficient and sustainable management of electric vehicle fleets.

IoT integrated with augmented reality can enable the creation of connected services for electric vehicles, offering a personalized driving experience to users. Specific software can facilitate charging procedures and provide additional and user-friendly information.

The application of optimization tools makes it possible to exploit vehicles as a source of flexibility for the electricity distribution network, favoring the integration of vehicles with networks and increasing their supply with energy from renewable energy sources. Electric vehicles can act as energy storage resources and provide demand response services to power grids. Using IoT, electric vehicles can be managed in a coordinated manner with renewable sources, optimizing the use of clean energy and contributing to grid stability.

In summary, the prospects in the IoT sector for smart grids are very promising. The use of IoT devices, real-time monitoring, automation, data analysis and integration of renewable energy sources and electric vehicles contribute to improving energy efficiency, resource management, sustainability and reliability of power grids.

PENDING EC APPROVAL



## 5 Comparison of IoT-NGIN technological outcomes and other next generation IoT technologies

The IoT-NGIN project addresses a collection of technological challenges for IoT application and service development. For each challenge, the project designs and implements certain advances over those features offered by selected baseline technologies the project leverages on. In this section, we identify those main features addressed by the project, the baseline technologies over which the project has built up new advances, and the novelties brought by the project.

In the following, for each technical WP, from WP2 to WP5, we describe the mapping between features and adopted baseline technologies, and report on the main novelties offered per features.

### 5.1 Enhancing IoT Underlying Technology

In this work-package, IoT-NGIN provides techniques for enhancing IoT underlying technology. In Table 2, we map the main functionalities with adopted baseline technologies.

The main feature domains addressed by IoT-NGIN for enhancing IoT underlying technology are (see D2.2 [4] and D2.3 [5]):

- Machine to machine communications,
- Machine - cloud - machine communications,
- IoT-centric dynamic management of 5G resources, and
- Secure Edge Cloud framework for IoT microservices

How the novelties brought by IoT-NGIN underlying technology are contributing to these domains is explained in the following paragraphs.

Table 2: Functionalities vs baseline technologies for WP2 - Enhancing IoT underlying technology.

Technologies				Functionalities													
				Machine to machine communications		Machine Cloud Communications			IoT-Centric dynamic management of 5G resources				Secure framework for microservices			Edge for IoT	Cloud IoT
				5G Coverage Extension	5G Energy Consumption Optimization	5G Infrastructure	5G Time Sensitive Networking	5G Network Slicing	5G Resource management	Unified and agnostic method to directly utilise 5G network features	5G MANO frameworks	Microservices migration process at the 5G edge cloud	Container technologies	Orchestration tools	Uni-kerne l		
Coverage Extension	FeD2D	Single Hop/MultiHop	5G	X													
			Wifi	X													
			Bluetooth	X													
	Relay Selection	Relay Selection	5G	X	X												
			Wifi														



			Blue tooth	X	X									
		Data Transmissi on	5G	X	X									
			Wifi	X	X									
			Blue tooth											
Energy Optimisation	Distance Detection				X									
	Relay power storage status				X									
5G Infrastructure	Base Stations					X		X						
	5G Core			X		X	X	X						
	UEs			X										
TSN	TSN bridge	Network-side TSN Translator					X				X			
		Device-side TSN Translator					X				X			
Network Slicing	5G Core Slicing							X	X		X			

	RAN Slicing					X	X			X			
Dynamic Resource Management	5G Connectivity & Device Management							X	X	X			
	Network Slice Management							X	X	X			
	Microservice Management Lifecycle							X	X	X			
Edge Cloud Framework	OS-level virtualization										X		
	Virtual Machines											X	
	Unikernel											X	X
	Host kernel Attacks										X		
	IoT NGIN Novelties	1		2			3				4		

## D1.4 - Continuous Technology Watch and Alignment

WP2 - Enhancing IoT underlying technology offers solutions, according to D2.1 [6], D2.2 and D2.3, that addresses these main domains:

- Machine to machine (D2D) communications: quoting D2.1, “D2D communications is a technique that allows a device to communicate directly with another device, without or partially going through the network infrastructure. In simple terms, D2D communications provide the connection between the two wireless devices either directly, when both devices are in line of sight (classical ad-hoc network), or by employing multi-hop routing techniques when there is a blockage between the devices (non-line of sight). When the devices are communicating with each other, data transmission can be shared among the devices in the network, thus tremendously mitigating the traffic on the overall core network at the expense of lower bandwidth since only one device is really connected to the network”.
- Machine - cloud - machine (MCM) communications: quoting D2.1, “The radio connectivity has been the major issue when considering MCM communications and there are several options focused primarily on cellular connectivity, Wi-Fi connectivity or customized/proprietary private-network connectivity. The availability of spectrum is one of the main showstoppers and over time there have been solutions spanning different frequencies. Some technologies take advantage of licensed and license-exempt spectrums to include cellular IoT, private LTE, private 5G, Wi-Fi and Low Power Wide Area (LPWA) IoT networks. The connectivity of MCM networks may vary depending on the implementation conditions and their usage scenario”
- IoT-Centric dynamic management of 5G resources, including:
  - 5G Connectivity and Device Management: “group encloses 5G capabilities such as device provisioning, device connectivity monitoring and management, device group management, etc”, as stated in D2.1,
  - Network Slice Management: “are mainly focused on the creation, configuration and deletion of network slices, where each network slice is formed of radio, cloud, and network parts”, as mentioned in D2.1,
  - Microservice Management: “provides functionalities for IoT services running in the edge-cloud. This includes management functionalities such as the creation or termination of new services, the management of existing services in terms of resource allocation (such as CPU or Memory) as well as the monitoring of the parameters of the services (e.g., status, resource consumption)”, as described in D2.1,
  - Service Migration: “enables a supervisory software or an IoT application directly to intelligently relocate an IoT service to either other nodes within the same edge-cloud or even to other nodes at different physical - locations.”, as commented in D2.1.
- Secure Edge Cloud framework for IoT microservices, including containers, orchestration tools and mostly focusing on unikernels: according to D2.2, “IoT-NGIN applications will be based on a set of micro-services. Consequently, each container usually deploys just one application, mainly using the network interface and CPU to handle requests. For each container, a traditional multi-processor, multi-tasking, multi-user operating system such as Linux as guest, would create a lot of overhead for small IoT-NGIN applications. Library Operating Systems (also known as Unikernels) are an attractive solution decreasing this overhead. The

## D1.4 - Continuous Technology Watch and Alignment

basic idea is to bundle the kernel with the application by linking them together and transforming the application and the kernel into a bootable application. Consequently, this realizes a single-address-space machine image only containing the necessary code for the application, thus reducing the memory footprint and boot time.

IoT-NGIN addresses these functionalities and brings advances as novelties which are describe in the following listing for the functionalities included in Table 2 (numbered from 1 to 4 in the last row):

1. Machine to machine (D2D) communications: As stated in D3.1, IoT-NGIN “proposes a simple, effective methodology for coverage extension by establishing device-to-device (D2D) communications between nodes outside the 5G cell coverage area and relays (devices connected to the cellular access point). It focuses on smartphones and has, as a design principle, to reject solutions that would require modifications on either the device itself or the operating system. The novelty of this approach is that candidate relays exchange several metrics with out-of-coverage nodes so that these later select the most suitable relay for some target performance. And, most importantly, without any intervention from the user”
2. Machine - cloud - machine (MCM) communications: from D3.1: “Several IoT applications, particularly those related to Industry 4.0, require deterministic temporal guarantees. Owners of these use cases are becoming more and more interested in using private LTE and 5G networks to increase their flexibility in configuring devices and communications without the need for cabling and its maintenance. IoT-NGIN addresses this objective by adapting existing Time Sensitive Network (TSN) solutions (originally designed for wired networks) to wireless industrial scenarios. Industrial IoT and machine process control are today based on wired automation, where data from devices and sensors are collected on edge servers and in a database. In a basic configuration, devices and sensors are connected to an edge server via private 5G networks. However, it is necessary to maintain the current transport and protocols used in wired connections to add new devices to the process and support their mobility over 5G networks. Therefore, existing industrial protocols must be used in both wired and wireless connections”.
3. IoT-Centric dynamic management of 5G resources: from D3.1, “A variety of APIs is already integrated into 5G products and services. A key challenge associated with these APIs is that they can be hard to understand for developers unfamiliar with 5G infrastructures and the mobile network domain. IoT-NGIN proposes a generic 5G resource management API to overcome this difficulty. This API will provide a more generic interface and simplify the usage of 5G resources. The specification of the IoT-NGIN 5G resource management API is an ambitious undertaking. It specifies new simplified resource management APIs for 5G. It can reduce the time and cost of implementing new services and applications using 5G communications by reducing the need for the involvement of 5G experts.”
4. Secure Edge Cloud framework for lot microservices: from d3.2, “The Unikernel approach promises to combine the advantages of existing approaches, based on containers and virtualization, to increase the secure isolation of the hosting kernel from running applications with minimal overhead. This approach promises to be an excellent fit for todays and future edge-clouds, where security as well as performance are vital. IoT-NGIN sees machine learning as a core topic for next-

generation IoT, thus we focus our efforts in developing unikernels for edge-clouds towards this field and are developing a flexible framework which enables developers to easily develop secure and performant unikernels for machine learning and AI in edge clouds"

## 5.2 Enhancing IoT Intelligence

In this work-package, IoT-NGIN provides techniques for enhancing the intelligence of IoT-based applications and services, delivered on IoT devices and EGDE infrastructures (see deliverables D3.3, D3.4). In Table 3, we map the main functionalities with adopted baseline technologies.

The main frameworks and services developed by IoT-NGIN for enhancing intelligence for IoT-based applications and services are the following (see D3.3 [7], D3.4 [8]):

- The ML as a Service (MLaaS) framework,
- The Online Learning Service,
- The Privacy Preserving Federated Learning (PPFL) framework,
- The Model Sharing service.

How these components are contributing to the novelty of IoT-NGIN for enhancing the intelligence of IoT-based applications and services is explained in the following paragraphs.

PENDING EC APPROVAL

Table 3: Functionalities vs baseline technologies for WP3 - Enhancing Intelligence.

Technologies	Functionalities (Enhancing Intelligence)															
	Learn models										Model Storage		Model Inference		Model Conversion	
	Data acquisition		Data Processing	Model Training / Evaluation												XAI
	Batch	Streaming		Batch	Online	Optimization	Federated	Data PP	Integrity Verification	Training / Evaluation Monitoring		CRUD	Integrity Verification	Batch	Online	
IoT Messaging (MQTT, Mosquitto)	X			X	X									X		
Streaming (Kafka)	X			X	X									X		
MLOps (Kubeflow, KServe, ML Frameworks, XAI)	X	X	X	X	X	X			X	X	X			X	X	
Workflows (Argo)				X			X									
Integration Framework (Camel-K)		X			X										X	
RL (Tensorforce)						X										

Storage (MinIO)	X			X	X	X	X				X		X	X	X	
Blockchain Ledgers (Quorum)							X		X			X				
Model Conversion (ONNX)															X	
Monitoring (Evidently Prometheus, Grafana, Tensorboard)										X						
Federated Learning (FLARE, TFF, Flower, PATE)							X	X								
IoT-NGIN Novelties	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

WP3 - Enhancing technology offers these main functionalities:

- To learn intelligence models from datasets collected from IoT devices. For this purpose, other functionalities are required:
  - Data acquisition: to gather IoT datasets used to train the intelligence models. It can be:
    - Batch acquisition: the complete dataset is provided at once,
    - Streaming acquisition: the dataset is fed continuously from sources to the training process.
  - Data processing: the dataset used to learn the model needs to be processed to a form required by the learning process.
  - Model training and evaluation, it can be:
    - Batch training: training is conducted once with a batch dataset,
    - Online training: training is an endless progressing process with datasets offered through streaming,
    - Optimization training: a special intelligence model is trained to find an optimal behavior for a managed system,
    - Federated training: a special case of batch training where several peers are collaborating together in training the model with local datasets. All these training cases also include these functionalities:
    - Training evaluation and monitoring: the training process is continuously monitored and evaluated for determining its performance (according to several metrics),
    - Model integrity verification: during the training process, the model integrity and its reproducibility is guaranteed with additional techniques.
  - Explainable AI (XAI), this functionality offers explanations about how the model learns from the provided dataset.
- To provide inference (or predictions) from learnt models, which offer intelligence to IoT applications and services. Inference can be:
  - Batch: inference is given for input datasets given on batches,
  - Online: inference is continuously provided upon request on data inputs given through streaming.
- To store learnt models for sharing and reuse. After the training process, learnt models can be stored in a central storage, to be shared among IoT devices and applications or to be reused (e.g., by using model transfer) to train other models. This functionality includes:
  - CRUD operations on models stored in the main storage,
  - Integrity verification of the models stored, to guarantee they have not been modified (without tracking) so they are reproducible (by training their architectures with the registered datasets).
- Model conversion permits to transform models trained with some ML frameworks to other ML execution platforms for a wider range of hardware compatibility.

IoT-NGIN addresses these functionalities and brings advances as novelties which are described in the following listing for the functionalities included in Table 2 (numbered from 1 to 16 in the last row):

1. Batch data acquisition is supported by the baseline components integrated into the MLaaS platform (i.e., Kubeflow, KServe). The novelty of MLaaS in this regard is



## D1.4 - Continuous Technology Watch and Alignment

to seamlessly offer both batch and online data acquisition in the same MLOps platform.

2. Online data acquisition is supported to gather streaming data from IoT devices in the MLaaS. This novelty is offered by using the integration framework Camel-K to connect streaming data sources to the MLaaS training processes deployed with KServe, in particular with the Online Learning service
3. Data processing is supported in MLaaS by using KServe Transformer. Novelty consists of integrating this feature in the holistic MLaaS solution
4. Batch training is supported by the technologies integrated into the MLaaS platform, through the Model Sharing services. Novelty consists on integrating Argo Workflows to train containerized model architectures within Kubernetes jobs, while guaranteeing the model integrity with smart contracts registered into blockchain ledgers.
5. Online training is offered as a novelty of the MLaaS platform compared to baseline technologies (e.g., Kubeflow, Kserve) which only offer batch training. Online learning collects datasets through online data acquisition and trains models in a continuous manner.
6. Optimization training is offered as a novelty to the MLaaS platform, by integrating RL frameworks such as Tensorforce. Nonetheless, this is a case-specific development, so each use case requires a specific optimization training implementation.
7. Federated learning offers as novelties a common specification for all integrated FL frameworks (i.e., TensorFlow Federated, Flower, Flare) and a common access point API to train models in federated manner.
8. Privacy preserving in FL was addressed by the PPFL framework. Main novelties are the implementation and integration of the PATE privacy preserving algorithm into FLARE FL framework and the investigation of the balance between privacy preservation and FL performance.
9. The model sharing services enable as main novelty the verification of the integrity of the trained model during the training process, by leveraging on blockchain ledger technology to store model architecture and training dataset metadata within a smart contract. This metadata is read-only and can be used to verify the integrity of the trained model.
10. Training evaluation and monitoring is a novelty for adopted MLOps baseline technologies, by integrating evaluating (i.e., Evidently, Tensorboard) and monitoring (i.e., Prometheus, Grafana) technologies into MLaaS, for tracking the model performance during the training and inference performance and data-drift detection on real-time.
11. Explainable AI has been included, as a novelty, into the MLaaS platform, as supported by KServe, but requiring case-specific XAI implementations.
12. Complete CRUD operations for data storage within MLaaS has been included as novelty, integrated with the model verification functionality, which guarantees the traceability and integrity of models stored, for sharing, into the MLaaS storage
13. As aforementioned, the integrity of all entities stored into the MLaaS storage, including datasets, and model architectures, is guaranteed with the adoption of smart contracts registered in blockchain ledgers.
14. Batch model inference is included into MLaaS by integrating the baseline technologies (i.e., KServe),

15. Online model inference is included into MLaaS, as a novelty, to support real-time streaming inference, by adopting the Camel-K bridge between IoT Gateways and KServe model serving.
16. As novelty, Model Sharing service enable the conversion of models, from backend ML frameworks (e.g., TF, Torch, etc.) into a common model representation (i.e., ONNX) that enables runtime inference over a wider range of hardware, which is quite suitable for IoT-based applications.

To conclude the MLaaS platform offers two high level novelties, namely:

- It offers a holistic MLOps platform for IoT-based applications and services based on the integration of open-source products, and
- It offers an agile framework, adopting GitOps, for the flexible customization of components, enabling the addition or removal of components

## 5.3 Enhancing IoT Tactile & Contextual Sensing/Actuating

In this work-package, IoT-NGIN provides techniques for enhancing the tactile and contextual sensing/actuating of IoT-based application and services, delivered on IoT devices and EGDE infrastructures (see deliverables D4.3 [9], D4.4 [10]). In Table 4, we map the main functionalities with adopted baseline technologies.

The main services developed by IoT-NGIN for enhancing the tactile and contextual sensing/actuating for IoT-based applications and services are the following (see D4.3, D4.4):

- IoT Device Discovery (IDD),
- IoT Device Indexing (IDI),
- IoT Device Access Control (IDAC),
- IoT AR/MR

How these components are contributing to the novelty of IoT-NGIN for enhancing the tactile and contextual sensing/actuating of IoT-based applications and services is explained in following paragraphs.

Table 4: Functionalities vs baseline technologies for WP4 - Enhancing IoT tactile and contextual sensing/actuating.

Technologies			Functionalities				
			IoT Device Discovery (IDD)		IoT Device Indexing (IDI)	IoT Device Access Control (IDAC)	IoT AR/MR Service
			Visual Methods	Non-Visual Methods	Management device related information and Support for the digital twin	Inter communication among IoT components and multi access criteria control	AR enhanced personalized IoT sensing and actuating
	Application Platforms	Unity, Vuforia-package					X
Computer Vision	Recognition Method	Convolutional Neural Network	X				
	Positioning Method	Homo-graphy	X				
	Specific Hardware Required	Camera	X				
Visible Light Positioning	Recognition Method	Visual Light Communication	X				

## D1.4 - Continuous Technology Watch and Alignment

	Positioning Method	Trilateration	X				
	Specific Hardware Required	LED Lamps Camera	X				
QR Codes	Recognition Method	Code Scanner	X				
	Specific Hardware Required	Camera	X				
Ultra-Wide Band Positioning	Recognition Method	Ultra-Wide Band		X			
	Positioning Method	Trilateration		X			
	Specific Hardware Required	UWB beacons UWB tag		X			
FIWARE Orion Context Broker	Infrastructure Technologies	Docker, Kubernetes, Helm			X		
	Communication Protocol Technologies	HTTP			X		
FIWARE IoT Agent	Infrastructure Technologies	Docker, Kubernetes, Helm			X		

	Communication Protocol Technologies	MQTT			X		
Historic Data Registry	Infrastructure Technologies	Docker, Kubernetes, Helm			X		
	Communication Protocol Technologies	HTTP			X		
API Kong Gateway	Security Methods	OAuth, JWT Token				X	
	Custom Plugins	Proximity, Keycloak, SSI (Self-Sovereign Identities)				X	
IoT NGIN Novelties			1	2	3	4	5

WP4 - Enhancing the tactile and contextual sensing/actuating technology offers these main functionalities:

- IoT Device Discovery (IDD): from D4.3, "The IoT Device Discovery component has three main functions:
  - Recognize objects that are contained inside a specific space from the signal received from different types of sensors. Position the objects recognized in a known coordinates system
  - Record the position of the objects together with the ID and the type of the object in the IoT Device Indexing module"
- IoT Device Indexing (IDI): from D4.3, "The IoT Device Indexing (IDI) module is a mechanism to store, keep track of and query a device's Digital Twin. A Digital Twin, while it does not have a definitive term in the literature, can be defined as the digital representation of a device's information. This copy can be used to access the device's data without having to come in direct contact with the device itself."
- IoT Device Access Control (IDAC): from D4.3, "Access control is of utmost importance in large IoT systems, with multiple services to be protected, a variety of users and different levels of access. The need for a highly efficient and transparent mechanism that allows multiple methods of authorization and authentication as per use case, is mandatory. The IoT Devices Access Control (IDAC) module of IoT-NGIN has been designed to handle the access to the resources of the IoT-NGIN framework, in a manner that does not imply the direct involvement of the clients or the devices per se. Through a single gateway URL, multiple services can be exposed in different paths and be protected according to the needs of the application. Users, instead of accessing the services directly, will just now need to make use of the IDAC API"
- IoT AR/MR: from D4.3, "Augmented and Mixed Reality (AR and MR) become promising solutions to visualize data from a rich variety of IoT sensors while keeping the focus on the associated real scenarios, and even to interact and actuate such sensors."

IoT-NGIN addresses these functionalities and brings advances as novelties which are describe in the following listing for the functionalities included in Table 3 (numbered from 1 to 5 in the last row):

1. Main novelties brought by IoT-NGIN to IDD are:
  - a. Visual Methods: Tracking and detection accuracy improvement. Positioning based on frequency identification and clustering. The component is provided to cover the QR scanning needs of UCs, based on SoTA methods and considering logging for security or other purposes
  - b. Non-visual methods: Positioning algorithm in NLOS (Non-Line-Of-Sight) situations or noisy scenarios
2. Main novelties brought by IoT-NGIN to IDI are:
  - a. Integrate with other systems of IoT-NGIN with developed APIs that allow the tool to communicate with other device management tools
  - b. Develop interfaces for device communication and metadata exchange.
  - c. Developed a reliable and secure communication between the physical device and its digital twin, allowing for seamless data exchange and control commands. Implemented advanced data analytics and machine

learning algorithms integration to optimize device performance based on the collected data from the digital twin,

3. Main novelty brought by IoT-NGIN to IDAC is the multi-access control system that can dynamically adjust access privileges based on user identity, device type, location, and other relevant factors to ensure secure and efficient data sharing among the IoT components.
4. Main novelties brought by IoT-NGIN to AR/MR are:
  - a. Mixed reality interface standards between machines and humans/employees
  - b. Increase the flexibility, interoperability, and scalability of manufacturing through hypermedia-based systems
  - c. Create and maintain a repository of AR/MR software components libraries and tools to support AR-IoT interaction.

PENDING EC APPROVAL

## 5.4 Enhancing IoT Cybersecurity & Data Privacy

In this work-package, IoT-NGIN provides techniques for enhancing the cybersecurity and data privacy of IoT-based application and services, delivered on IoT devices and EGDE infrastructures (see deliverables D5.2 to D5.5 [11], [12], [13], [14]). In Table 5, we map the main functionalities with adopted baseline technologies.

The main frameworks and services developed by IoT-NGIN for enhancing the cybersecurity and data privacy of IoT-based applications and services are the following (see D5.2 to D5.5):

- The Semantic Twin,
- The Decentralized Interledger Bridge (DIB),
- The Verifiable Credential (VC) based Access Control (AC),
- The Quick Response (QR) code and Global Standards 1 (GS1) digital-link discovery mechanism,
- The GAN-based dataset generator,
- The Malicious Attach detector,
- The IoT Vulnerability Crawler,
- The Moving Target Defence.

How these components are contributing to the novelty of IoT-NGIN for enhancing the cybersecurity and data privacy of IoT-based applications and services is explained in following paragraphs.

PENDING EC APPROVAL



Table 5: Functionalities vs baseline technologies for WP5 – Enhancing IoT Cybersecurity and data privacy.

Technologies	Functionalities							
	GAN-based dataset generator (DDG)	Malicious Attack Detector (MAD)	IoT Vulnerability Crawler (IVC)	Moving Target Defense (MTD)	Semantic Twin (ST)	Decentralized Interledger Bridge (DIB)	Self-Sovereign Identity Technologies	
	Semantic Twin (ST)	Decentralized Interledger Bridge (DIB)	Self-Sovereign Identity Technologies		GAN-based dataset generator (DDG)	Malicious Attack Detector (MAD)	Verifiable Credential (VC) - based Access Control (AC) for constrained devices	QR (Quick Response) code and GS1 (Global Standards 1) digital link-based discovery mechanisms
Twin document server					X			
Access Management Proxy Server					X			
DID Resolver					X			X
GS1 Digital Link Resolver					X			X
DLT	X				X	X		

DSM						X		
IAA Proxy							X	
Supervised/Unsupervised ML	X	X						
Continuous Delivery (CD) - Argo			X	X				
HoneyPot				X				
Workflow Framework - Argo Workflows			X	X				
Container management - Kubernetes, Helm			X	X				
SQL/NonSQL DBMS			X					
IoT-NGIN Device Indexing			X					
IoT-NGIN Novelties	1	2	3	4	5	6	7	8

WP5 - Enhancing the cybersecurity and data privacy offers these main functionalities:

- The Semantic Twin, according to D5.5, "Semantic Twins give context and meaning to Digital Twins and real-world entities by providing information about the services of real-world entities and their Digital Twins in a unified human and machine-readable format."
- The Decentralized Interledger Bridge (DIB), according to D5.5, "the decentralized DIB provides the shared trust among a consortium of participants for interledger transactions, while improving the resiliency of the interledger data transfer via redundancy of nodes".
- The Verifiable Credential (VC) based Access Control (AC), according to D5.5, "Verifiable Credentials allow flexible and privacy-preserving access control solutions. E.g., suppose there is a factory that has outsourced the maintenance to a separate company. The technician working for the maintenance company needs to receive temporary access to factory premises and to certain machines there, but the factory does not need to learn about the technician's real identity or whether the technician is the same as the one who visited the factory previously."
- The Quick Response (QR) code and Global Standards 1 (GS1) digital-link discovery mechanism, according to D5.5, "A GS1 Digital Link converts a barcode, either one or bi-dimensional, into a web address that contains the information on a product the barcode refers to. GS1 digital links are used to discover the locations of the Digital and Semantic Twin of an entity Triplet."
- The GAN-based dataset generator, according to D5.2, "Data generation can be achieved with multiple methods such as data duplication or GANs. Regarding the latter case, the GAN algorithm can learn a dataset's distribution and later be leveraged for data generation. The trained GAN model can be used to create synthetic data (tabular or images) that can consequently be manipulated concerning a malicious goal. Therefore, this generated data can be exploited to create model and data poisoning attacks in a FL system."
- The Malicious Attack detector (MAD), according to D5.5, "MAD is an advanced tool that can identify and block malicious activities within the federated learning system. We introduce the label flipping mitigation technique that aims to eradicate the effects of such attacks. This technique relies on the assumption that the federated server has a small, clean dataset and can train the global model for a few rounds locally after the federated training process has ended. Together with the label flipping mitigation technique, MAD provides an extra layer of protection against cyber threats, thereby enhancing the overall security of the federated learning environment"
- The IoT Vulnerability Crawler, according to D5.2, "is a structure constructed by multiple components and its purpose is to offer proactive security measures in an IoT-device network by scanning each device for potential vulnerabilities. IVC offers three different modes of vulnerability scanning executions:
  - on demand
  - ii) on first appearance
  - iii) on a time-scheduled basis"
- The Moving Target Defence, according to D5.5, "is a defense mechanism that alleviates an increasing number of threats that target IoT and FL systems and ecosystems... MTD Honeypots framework constitutes a honeypot-based technical solution that also incorporates dynamic configuration capabilities. In the IoT-NGIN project, the MTD term refers to the ability of the framework to alter the provided functionality and network configuration based on some input. The above-mentioned

capability is considered an effective countermeasure against temporary cyberattacks. This is because the honeypots that are deployed in an IoT network are constantly changing their associated network and system configurations, which in turn makes the established honeypots hard to be detected by an adversary. At the same time, the MTD Honeypots framework succeeds in decreasing the attackers' knowledge over an IoT system.

IoT-NGIN addresses these functionalities and brings advances as novelties which are described in the following listing for the functionalities included in Table 4 numbered from 1 to 8 in the last row):

1. Main novelties brought by IoT-NGIN to the GAN-based dataset generator are:
  - a. Supports GAN training on limited image/tabular dataset
  - b. Backdoor attack in FL targeting a global classification model with limited number of malicious participants
2. The main novelty brought by IoT-NGIN to the Malicious Attach Detector is:
  - a. More effective mitigation of backdoor/network attacks in FL compared to literature
3. The main novelty brought by IoT-NGIN to the IoT Vulnerability Crawler is:
  - a. Flexible mechanism to integrate scans for known vulnerabilities in networked assets
4. The main novelty brought by IoT-NGIN to the Moving Target Defense is:
  - a. Flexible automated honeypot deployment platform, integrating diverse honeypots for known attacks, basing MTD on IP randomization.
5. The main novelty brought by IoT-NGIN to the Semantic Twin is:
  - a. Enables the automated deployment, discovery and utilization of Triplets, that provides more trustworthy services in an easier to use format,
6. The main novelty brought by IoT-NGIN to the Decentralized Interledger Bridge is:
  - a. The decentralization improves
    - i. trustworthiness, by trusting the consortium of parties running the nodes forming the bridge,
    - ii. resiliency, as nodes act as backups for each other, so another node will automatically take over for a failed node, and
    - iii. scalability, by adding more nodes to the bridge, the throughput of the bridge can be increase,
7. Main novelties brought by IoT-NGIN to the VC based AC are:
  - a. Demonstrates low-latency on-device access control,
  - b. This solution has been integrated into the WP4 Access Control component,
8. The main novelty brought by IoT-NGIN to the QR code and GS1 digital-link discovery mechanism is:
  - a. Facilitates the easy deployment and management of Triplets

## 5.5 List of IoT-NGIN Technological outcomes

Table 6: List of IoT-NGIN Technological Outcomes.

No.	KER	Description	Current TRL	Owned by Partner(s)	Nature of the KER
1	Industrial 5G Core with network slice manager	The 5GC includes network slice manager to separate devices and traffic with different requirements i.e. IoT traffic from consumer data. The 5GC includes features such as 5GLAN, TSN required specifically for private installation and integration with industrial infrastructure.	4	CMC	Software
2	IoT-NGIN 5G Resource Management API	Open 5G Resources Management API to enable IoT devices to access the IoT-NGIN resources, providing connectivity, along with its native secure, tactile, low-latency and reliable connectivity facilities.	3	RWTH	Software and API subcomponent
3	Enhance IoT/5G FeD2D	D2D API which allows enhanced connectivity of IoT devices in 5G networks, implementing an advanced relay selection strategy, based on experimental evaluation of D2D links, as well as information sharing with the underlying infrastructure	4	SU, eBOS	Software
4	Secure Edge Cloud Framework	An innovative “by design” framework using the most advanced programming language in security (Rust) and unikernels to support secure, deployable and scalable edge cloud execution framework for IoT focused micro-services.	3	RWTH	Software
5	ML as a Service platform	MLaaS platform offering AI scientists and developers Data Management, ML training, Model Sharing and Prediction as a service, offering APIs and/or SDK to train and optimize AI models, supporting self-learning capabilities	6	CAP	Software/prototype

6	ML Online Learning framework	ML Online Learning enables the online training of ML by the continuous feeding of training datasets through streaming, as well as online inference	6	ATOS	Software/prototype
7	Model Sharing, Model Translation and Zero Knowledge Verification framework	Model Sharing, Model translation and Zero Knowledge Verification service ecosystem enables the verified training and storage of ML models. Verification and reproducibility of the ML training process is guarantee by smart contracts registered within private and public blockchain ledgers.	5	ATOS	Software/prototype
8	Privacy preserving federated ML	The Privacy-preserving Federated Learning framework allows the development of more efficient ML models, which are trained considering data from multiple sources with increased privacy guarantees, without disclosing the data and protecting the information communicated, which could lead to data disclosure.	5	INTRA, SYN	Software
9	Semantic twin	Semantic twin document provides a semantic description of the digital twins and the related real-world entities, e.g., API endpoints, identity, relations to other twins, etc., incorporating digital Self-Sovereign Identities and SAREF ontologies	5	ABB, AALTO	Software and methodology
10	AI-based object recognition algorithm using computer vision	The AI-based algorithm processed images to identify Synelxis box in the field, as well as smart energy charging stations in the city.	5	EBOS	Software/Prototype
11	IoT Device Discovery	IoT tactile and contextual sensing/actuation, based on device discovery using computer vision and deep learning methods	5	I2CAT	Software/Hardware (Localization submodules of the IoT Device

		through real-time video analysis in an XR environment, a novel easy-to-manage access rights system and an IoT-AR assets repository			Discovery based on computer vision)
12	Moving Target Defence (MTD) network of Honeypots	The Moving Target Defence (MTD) can be exploited as part of an integrated cybersecurity solution or as a stand-alone cyber-defence mechanism offered either as a product or as a service that also includes the IoT network analysis process for added value. The latter, enables the option for providing a domain specific service.	5	INTRA	Software
13	IoT Vulnerabilities Crawler	IoT Vulnerability Crawler able to identify vulnerable IoT nodes from network security perspective, leveraging on awareness of known vulnerabilities appearing in relevant well-known open repositories.	6	SYN	Software
14	Malicious Attack Detector	Malicious Attack Detection against model and data poisoning attacks in Federated Learning networks. The approach employs ML techniques via Generative Adversarial Networks to learn and detect poisoning attacks in malicious nodes.	5	INTRA	Software
15	Privacy-preserving self-sovereign identity solutions	Proof-of-concept prototypes demonstrate how self-sovereign identities can be used to increase trust in IoT-applications while still effectively protecting the privacy of different parties.	4	AALTO	Software
16	Decentralised Interledger Bridge	Interlinking different types of distributed ledgers with atomic transactions enables new types of services and helps overcome the limitations of individual ledgers.	4	AALTO	Software

17	ML-based precision agriculture modules	A set of modules appropriate for precision agricultural solutions, including ML formulations which support crop disease prediction and aerial spraying	5	SYN	Software
18	Crop harvesting assisting framework	The crop harvesting assisting framework, built on top of IoT-NGIN ML tools, integrates mobile robots moving autonomously as carriers of harvested crops with the accompanying application supporting monitoring and management of the crop harvesting assisting process.	5	SYN	Prototype
19	AR Based Maintenance Services	These AR based services are part of the AR/VR module that instantiate different functionalities. For example, some functionalities will enable the IoT-NGIN architecture to present the information from related IoT sensors (e.g., the surrounding or requested ones) via Augmented Reality and even to actuate them.	4	ENG	Software and Services
20	Blockchain based services	A distributed ledger is a type of database that is shared, replicated, and synchronized among the members of a decentralised network. Unlike traditional databases, distributed ledgers have no central data store or administration functionality. The distributed ledger records the transactions. Each network participant holds a copy of the ledger and reaches an agreement on the updates to the records in the ledger.	4	ENG	Software and Services
21	IoT Device Indexing	The IoT Device Indexing component enables the creation of a repository of IoT devices, allowing quickly querying about their status, basic characteristics and associated monitoring or other regularly updated information, thus indexing both the physical and digital twin of IoT devices.	6	SYN	Software and Services



22	IoT devices access control	Security middleware between IoT devices and services, enabling pervasive security based IoT access control, extending static access rights by managing user rights by physical proximity or visibility as a flexible security and policy management API gateway	6	OPT, SYN	Software and Services
23	Cloud Native support for the Slice Manager	Slicing & Orchestration Engine (SOE) is a management framework for private 5G networks. It includes a Slice Manager (SM) module, an ETSI NFV orchestrator (ETSI OSM), a multi-vendor RAN element manager, and a telemetry collection framework. SOE is responsible for the LifeCycle Management (LCM) of network slices and the orchestration of associated vertical services running atop each network slice. Whenever a slice is requested, the SM module creates compute, radio, and network chunks, and then stitches them together to form the requested network slice, enabling network services to run on top of the created slice. Throughout the project's lifetime, i2CAT extended the SM module by adding support for the Kubernetes API as a Virtual Infrastructure Manager (VIM), supplementing its existing support for OpenStack. This enhancement enables the module to perform LCM of Cloud-Native Functions (CNFs).	5	I2CAT	Software and Services

## 5.6 IoT Technological Maps & Direct Comparison to IoT-NGIN Outcomes

### 5.6.1 Enhancing IoT Underlying Technology

The following graph shows the technological sectors concerning WP2 activities. There are four main areas, the "Machine to Machine communication", "IoT-centric dynamic management of 5G resources", "Machine Cloud Machine Communications", and "Secure Edge Cloud framework for IoT micro-services". For each of them progress and integrations have been made in different areas. The technologies used are coverage extension, energy optimization, 5G infrastructure, TSN, Network slicing, Dynamic resource management and edge-cloud framework.

WP2 activities produced several enhancements to 5G technologies, in order to progress in terms of technological maturity and commerciality. The main contributions covered four areas: coverage extension, support of time-critical applications, enhanced exposure of 5G resources, and security.

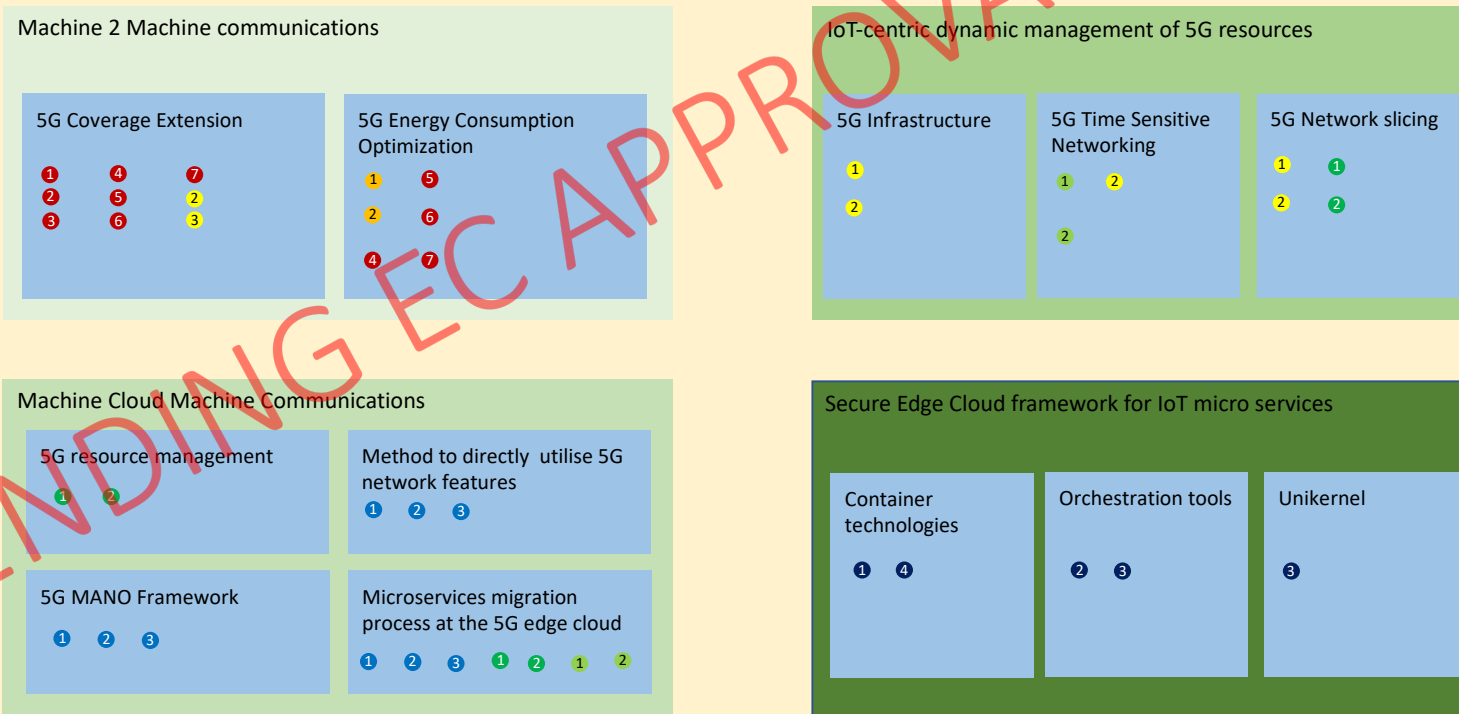
Concerning "Coverage extension" a simple methodology for coverage extension by establishing device- to-device (D2D) communications between nodes outside the 5G cell coverage area and relays has been developed. The originality of the approach is that candidate relays exchange several metrics with out-of-coverage nodes so that these later select the most suitable relay for some target performance, without any intervention from the user. Since this approach leads to a proximity service, it's possible to implement algorithms to meet the requirements of different scenarios that hotspot solutions cannot satisfy.

Concerning "Support of time-critical applications" leveraging the growing demand for private LTE and 5G networks to perform particular industrial applications. Existing Time Sensitive Network (TSN) solutions were used. The work has focused on architectures and prototype implementations of this functionality, which has already been defined in 3GPP standards for 5G networks.

In the "Enhanced exposure of 5G resources" area, one of the current states of the art challenge is the difficulty of understanding the existing APIs for unexpert. So, a generic 5G resource management API has been used to overcome this complexity. The API focuses on three different groups of relevant capabilities: 5G connectivity and device management, network slice management, and microservice lifecycle management.

Finally, in the "security" area, we faced a lack of isolation between the host operating system and the containerized application. Indeed, a security vulnerability in the container runtime directly exposes the host kernel to attacks or the other containers, which are managed by the runtime. A possible solution is through virtual machines (VM), that increase the isolation, but requires additional kernel in the VM and induce a lot of overhead. Based on these considerations, an Unikernel approach has been followed, that allow a good isolation with minimal overhead.

## WP2



COVERAGE EXTENSION	ENERGY OPTIMIZATION	5G INFRASTRUCTURE	TSN	NETWORK SLICING	DYNAMIC RESOURCE MANAGEMENT	EDGE CLOUD FRAMEWORK
<ul style="list-style-type: none"> <li>1 FeD2D: 5G</li> <li>2 FeD2D: WiFi</li> <li>3 FeD2D: Bluetooth</li> <li>4 Relay Selection - authentication: Bluetooth</li> <li>5 Relay Selection - authentication: 5G</li> <li>6 Relay Selection - transmission: 5G</li> <li>7 Relay Selection - transmission: WiFi</li> </ul>	<ul style="list-style-type: none"> <li>1 Distance detection</li> <li>2 Relay power storage status</li> </ul>	<ul style="list-style-type: none"> <li>1 Base Stations</li> <li>2 5G Core</li> <li>3 UEs</li> </ul>	<ul style="list-style-type: none"> <li>1 Network-side TSN Translator</li> <li>2 Device-side TSN Translator</li> </ul>	<ul style="list-style-type: none"> <li>1 5G Core Slicing</li> <li>2 RAN Slicing</li> </ul>	<ul style="list-style-type: none"> <li>1 5G Connectivity &amp; Device Management</li> <li>2 Network Slice Management</li> <li>3 Microservice Lifecycle Management</li> </ul>	<ul style="list-style-type: none"> <li>1 OS-level virtualization</li> <li>2 Virtual Machines</li> <li>3 Unikernel</li> <li>4 Host kernel Attacks</li> </ul>

Figure 37: Technological Map on the Enhancement of IoT Underlying Technologies.

Table 7: Main technological advancements towards the enhancement of IoT Underlying Technology.

Technology	Advancements by IoT-NGIN
Coverage extension	The originality of IoT-NGIN approach is that candidate relays exchange several metrics with out-of-coverage nodes so that these later select the most suitable relay for some target performance without any intervention from the user.
Support of time-critical applications	We are addressing this challenge by adapting existing Time Sensitive Network solutions to wireless industrial scenarios.  These ongoing investigations have focused on both the theoretical use of the functionality and the potential deployment of the functionality in a live LTE or 5G network at trial sites. We have developed multiple prototypes relevant for the industry and agricultural sectors.
Enhanced exposure of 5G resources	An original API has been developed to provide a more generic interface and simplify the usage of 5G resources. It specifies new simplified resource management APIs for 5G. It can reduce the time and cost of implementing new services and applications using 5G communications by reducing the need for the involvement of 5G experts.
Security	The Unikernel approach promises have an increased isolation with minimal overhead. This approach promises to be an excellent fit for todays and future edge-clouds, where security as well as performance are vital.

## 5.6.2 Enhancing IoT Intelligence

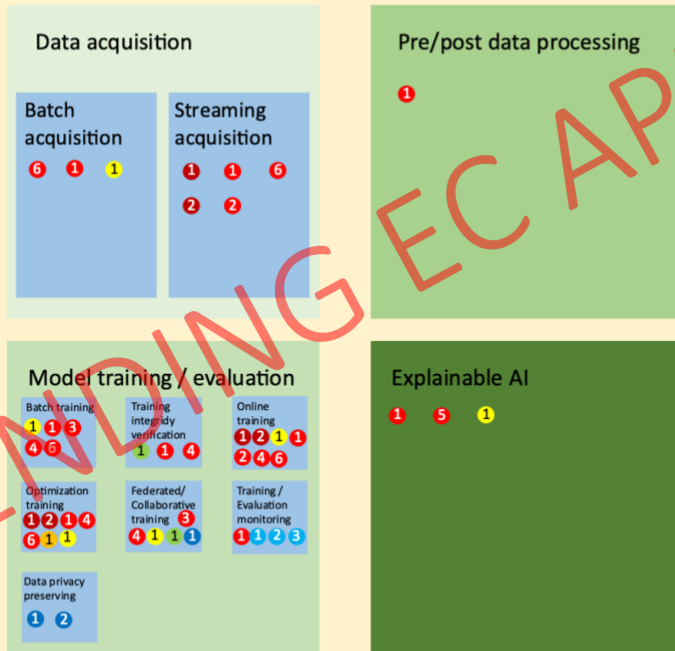
The figure shows the technological sectors touched by the WP3 activities, with the different tools used divided by area. It should be noted that there are two main areas, the "Learn models" and the "Serve models" and for each of them progress has been made in different areas. The technologies used are stream technologies, MLOPS, reinforcement learning, storage, blockchain, conversion, monitoring and federated learning.

WP3 consists of two main blocks, one concerning Machine Learning as a Service (MLaaS) and the other concerning privacy-preserving Federated Learning. In terms of MLaaS, a common holistic platform was realised, called ML operations platform. This platform combines some open-source implementations with additional services. The services include ML model storage by integrating MinIO, Rook and Ceph; Data storage as PostgreS and InfluxDB; Data acquisition as MQTT, Kafka, Camel-k; IAM/AAI Keycloak and CI/CD installation based on Argo-CD. In addition, modules for online model training, model translation and zero-knowledge model verification based on BlockChain have been added.

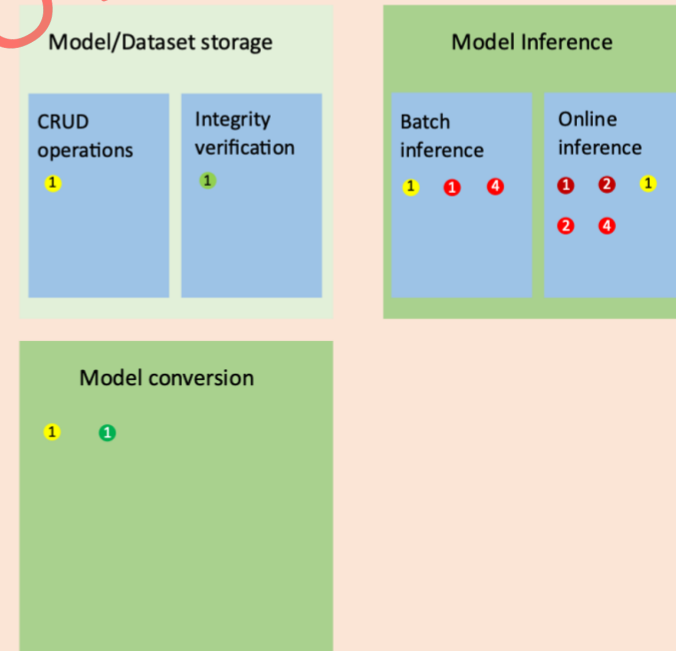
Concerning the Privacy-Preserving Federated Learning (PPFL) Framework, locally trained ML models are aggregated in a 'server' node and shared to the 'clients', without disclosing data to each other, while enforcing privacy preservation during model exchange. The PPFL Framework provides easy access to diverse federated learning approaches, able to operate for different applications. In particular the following frameworks are integrated and enhanced: NVIDIA FLARE, FLOWER and Tensorflow Federated. In some of the areas the contribution of IoT-NGIN has been more innovative and the following table shows the main contributions with respect to the state of the art.

## WP3 - Enhancing Intelligence

### Learn models



### Serve Models



STORAGE

STREAM TECHNOLOGIES	MLOPS	REINFORCEMENT LEARNING	STORAGE	BLOCKCHAIN	CONVERSION	MONITORING	FEDERATED LEARNING
<ul style="list-style-type: none"> <li>1 MQTT: Mosquitto</li> <li>2 Streaming Framework Kafka</li> </ul>	<ul style="list-style-type: none"> <li>1 KServe</li> <li>2 Integration Framework Camel-K</li> <li>3 Argo Workflows</li> </ul>	<ul style="list-style-type: none"> <li>1 TensorForce</li> </ul>	<ul style="list-style-type: none"> <li>1 K8S Object Storage MiniIO</li> </ul>	<ul style="list-style-type: none"> <li>1 Ladders: quorum</li> </ul>	<ul style="list-style-type: none"> <li>1 ONNX</li> </ul>	<ul style="list-style-type: none"> <li>1 ML Monitoring evidently</li> <li>2 Monitoring Engine Prometheus</li> <li>3 Visualization Grafana, Tensorboard</li> </ul>	<ul style="list-style-type: none"> <li>1 Federated Learning Frameworks ( FLARE, TFF, Flower)</li> <li>2 Privacy preserving methods (PATE)</li> </ul>
	<ul style="list-style-type: none"> <li>4 ML Frameworks</li> <li>5 XAI Frameworks</li> <li>6 MLOps Frameworks Kubeflow</li> </ul>						

Figure 38: Technological map on the Enhancement of IoT Intelligence.

Table 8: Main technological advancements towards the enhancement of IoT intelligence.

Technology	Advancements by IoT-NGIN
Data acquisition - Batch acquisition	It integrates baseline technologies in MLaaS platform
Data acquisition - Streaming acquisition	It integrates baseline technologies in MLaaS platform. It leverages Camel-K to connect Streaming data sources to MLaaS services deployed with KServe: online learning, optimization learning
Pre/Post data processing	It integrates baseline technologies in MLaaS platform
Model training/Evaluation - Batch training	It integrates baseline technologies in MLaaS platform. It leverages Argo Workflows to train models with containers provided by users with Blockchain Ledger based integrity verification
Model training/Evaluation - Training integrity verification	During the batch training, it guarantees the integrity of the overall training process, leveraging Blockchain ledger technology
Model training/Evaluation - Online training	It integrates baseline technologies in MLaaS platform. It uses streaming datasets to online train ML models on continuous basis with monitoring validation
Model training/Evaluation - Optimization training	It integrates baseline technologies in MLaaS platform. It gives support for optimization training with monitoring
Model training/Evaluation - Federated/ Collaborative training	It integrates baseline Federated learning frameworks with a single access point API and Argo Workflows for peer-training
Model training/Evaluation - Training/Evaluation monitoring	It integrates baseline technologies in MLaaS platform for online and optimization training
Model training/Evaluation - Data privacy preserving	It integrates privacy preserving methods for collaborative training in federated learning (i.e., PATE method integrated on Flower)
Model/Dataset storage - CRUD operations	It integrates baseline technologies in MLaaS platform, offering a single access API for batch, online and federated learning, supporting integrity verification with Blockchain ledger contracts
Model/Dataset storage - Integrity verification	It guarantees the integrity of stored artefacts, including datasets and ML models
Model/Dataset storage - batch inference	It integrates baseline technologies in MLaaS platform
Model/Dataset storage - online inference	It integrates baseline technologies in MLaaS platform, supporting requesting inference from streaming sources
Model conversion	It integrates baseline technologies in MLaaS platform, supporting conversion of ML models to ONNX, storage in central MLaaS storage with integrity guarantee.

### 5.6.3 Enhancing IoT Tactile & Contextual Sensing/Actuating

The table shows the technological sectors touched by the activities of WP4, with the different tools used divided by area. It should be noted that there are four main areas, the "IoT Device Discovery", the "IoT Device Access control", the "IoT Device Indexing" and the "IoT AR/MR Service". There are also the "Serve models" and for each of them steps have been taken forward in different fields. The technologies used are the application platform, computer vision, visible light positioning, QR codes, ultra-wide band positioning, fiware orion, fiware IoT agent, historic data registry, API kong gateway.

WP4 provides innovations in various technologies, the main are IoT Device Discovery and Indexing, IoT Device Access Control and IoT Device Augmented Reality actuation.

Concerning IoT Device Discovery and Indexing, fast and versatile software components have been developed for recognition, positioning and indexing of different objects. Different recognition methods, both visual and non-visual, are integrated in the Discovery module and the main advancements concern the reduction of latency in the detections, improvements in the accuracy and the robustness of the methods. The modules recognized in the IoT Discovery are registered in the IoT Indexing Module, with several information per device and the main novelties are the ability of the IoT Device Indexing of supporting historical data services, implementing on Helm chart and registering the position of different object.

The IoT Device Access Control service has been implemented to handle in a flexible way the access to the resources of the Project. The module is implemented as a flexible Ingress Gateway enforcing chained access control methods, following different access control mechanisms which are implemented as plugins: Proximity plugin, OpenID Connect Authentication plugin and Self Sovereign Identities plugin.

The IoT Device Augmented Reality actuation is a model able to communicate with different devices, framework and tools. The main novelty is that a set of APIs have been created, that will allow the different AR tools to interact with the IoT Device Indexing module.

In some of the areas the contribution of IoT-NGIN has been more innovative and the following table shows the main contributions with respect to the state of the art.



## WP4

### IoT Device Discovery (IDD)

#### Visual Methods

- 1 2 3 1 2 3
- 1 2

#### Non Visual Method

- 1 2 3

### IoT Device Access Control (IDAC)

Inter communication among IoT components and multi access criteria control

- 2 3 4 5

### IoT Device Indexing (IDI)

Management device related information and Support for the digital twin

- 1 2 3 4 1 2 3 4 1 2 3 4

### IoT AR/MR Service

AR enhanced personalized IoT sensing and actuating

- 1 2

APPLICATION PLATFORM	COMPUTER VISION	VISIBLE LIGHT POSITIONING	QR CODES	ULTRA WIDE BAND POSITIONING	FIWARE ORION	FIWARE IOT AGENT	HISTORIC DATA REGISTRY	API KONG GATEWAY
<ol style="list-style-type: none"> <li>1 Unity</li> <li>2 Vuforia-package</li> </ol>	<ol style="list-style-type: none"> <li>1 Convolutional Neural Network</li> <li>2 Homo-graphy</li> <li>3 Camera</li> </ol>	<ol style="list-style-type: none"> <li>1 Visual Light Communication</li> <li>2 Trilateration</li> <li>3 LED Lamps Camera</li> </ol>	<ol style="list-style-type: none"> <li>1 Code Scanner</li> <li>2 Camera</li> </ol>	<ol style="list-style-type: none"> <li>1 Ultra wide Band</li> <li>2 Trilateration</li> <li>3 UWB beacons – UWB tag</li> </ol>	<ol style="list-style-type: none"> <li>1 Docker</li> <li>2 Kubernetes</li> <li>3 Helm</li> <li>4 MQTT</li> </ol>	<ol style="list-style-type: none"> <li>1 Docker</li> <li>2 Kubernetes</li> <li>3 Helm</li> <li>4 MQTT</li> </ol>	<ol style="list-style-type: none"> <li>1 Docker</li> <li>2 Kubernetes</li> <li>3 Helm</li> <li>4 MQTT</li> </ol>	<ol style="list-style-type: none"> <li>1 oauth</li> <li>2 Token jwt</li> <li>3 Proximity</li> <li>4 Keycloak</li> <li>5 SSI (self Sovereign Identities)</li> </ol>

Figure 39: Technological map on the Enhancement of IoT Tactile & Contextual Sensing/Actuating.



Table 9: Main technological advancements towards the enhancement of IoT tactile & contextual sensing/actuating.

Technology	Advancements by IoT-NGIN
IoT Device Discovery - Visual Methods	Tracking and detection accuracy improvement. Positioning based on frequency identification and clustering. The component is provided to cover the QR scanning needs of UCs, based on SoTA methods and considering logging for security or other purposes
IoT Device Discovery - Non-Visual Methods	Positioning algorithm in NLOS (Non-Line-Of-Sight) situations or noisy scenarios
IoT Device Indexing - Management device related information and Support for the digital twin	<ul style="list-style-type: none"> <li>• Integrate with other systems of IoT-NGIN: Developed APIs that allow the tool to communicate with other device management tools</li> <li>• Develop interfaces for device communication and metadata exchange.</li> <li>• Developed a reliable and secure communication between the physical device and its digital twin, allowing for seamless data exchange and control commands. Implemented advanced data analytics and machine learning algorithms integration to optimize device performance based on the collected data from the digital twin.</li> </ul>
IoT Device Access Control - Inter communication among IoT components and multi access criteria control	Multi-access control system that can dynamically adjust access privileges based on user identity, device type, location, and other relevant factors to ensure secure and efficient data sharing among the IoT components.
IoT AR/MR Service - AR enhanced personalized IoT sensing and actuating	<ul style="list-style-type: none"> <li>• Designing mixed reality interface standards between machines and humans/employees</li> <li>• Increase the flexibility, interoperability, and scalability of manufacturing through hypermedia-based systems</li> <li>• Create and maintain a repository of AR/MR software components libraries and tools to support AR-IoT interaction.</li> </ul>

## 5.6.4 Enhancing IoT Cybersecurity & Data Privacy

The table shows the technological sectors touched by the WP5 activities, with the different tools used divided by area. There are seven main areas, "Semantic Twin", "Decentralized Interledger bridge", "Self-sovereign Identity Technologies" and "GAN-based dataset generator", "Malicious Attack Detector", "IoT Vulnerability Crawler" and "Moving Target Defense". For each of them, progress has been made in different fields compared to the state of the art and different technologies have been tested. The technologies used are the twin document server, the access management proxy server, the DID Resolver, the GS1 Digital Link Resolver, DLT, DSM, IAA Proxy, Supervised/Unsupervised ML, Continuous Delivery - Argo, HoneyPot, Workflow Framework - Argo workflow, Container management - Kubernetes, Helm, SQL/nonSQL DBMS, IoT-NGIN Device Indexing.



Figure 40: Technological map towards the Enhancement of IoT Cybersecurity & Data Privacy.

WP5 deals with cybersecurity risks and data privacy issues related with IoT devices operation. The main contributions to the sector are some innovative tools and components developed in the Project. The Generative Adversarial Network (GAN) based IoT attack dataset generator component generates high-value synthetic datasets of network attacks, do not requiring big amounts of real data. The Malicious Attack Detector (MAD) is able to identify attacks in on-device Federated Learning, based on ML anomaly detection models. The IoT vulnerabilities crawler identifies common vulnerabilities in distributed IoT systems, it's a scalable module and additional vulnerabilities can be detected with minimum effort. Finally, the Moving Target Defense (MTD) network of Honeypots allows exploration of attackers' behavior, exploiting IoT systems' vulnerabilities.

Table 10: Main technological advancements towards the enhancement of IoT Cybersecurity & Data Privacy.

Technology	Advancements by IoT-NGIN
Generative Adversarial network based IoT attack dataset generator	The GAN Generator is able to create close-to-real synthetic datasets for both tabular data and images, starting with a small amount of data, proving useful for training attack detection models targeting both network and data.
Malicious Attack Detector	It's based on ML anomaly detection models useful for both network attacks and data poisoning.
IoT vulnerability Crawler	It identifies common vulnerabilities in distributed IoT systems. It features a distributed cloud-native architecture leveraging service-oriented plugins, which ensure scalability and extensibility.
Moving Target Defense network of Honeypots	MTD dynamically changes the attack surface to continuously increase complexity and confuse the attacker, thus preventing the system vulnerabilities from being exploited. The MTD network of Honeypots can be used to mimic vulnerabilities identified by the IoT vulnerabilities crawler and can provide useful feedback to the vulnerability and threat modelling.

## 6 Conclusions

The deliverable presented here is a comprehensive response to the activities carried out in Task 1.4, titled "Continuous Technology Watch and Alignment on Next Generation IoT Advancements," which is part of Work Package (WP) 1, named "Next Generation IoT Requirements & Meta-Architecture." The purpose of this report is to highlight the outcomes from WP1 and shed light on the progress made in IoT-NGIN (Next Generation IoT) project.

The report begins by providing insights into the technological survey conducted during the course of WP1. It outlines the methodology employed to carry out the survey and presents the results and analysis of the contributions obtained. The primary objective of this survey was to gain a comprehensive understanding of the specific needs and opportunities within the IoT-NGIN sector. Moreover, the survey aimed to evaluate how the IoT-NGIN project's accomplishments compare and differ from other ongoing next-generation IoT technological advancements in the market.

Building on the initial technology watch snapshot and the technological innovations made during the IoT-NGIN project, the report then proceeds to conduct a direct comparison of IoT-NGIN's outcomes with the current state-of-the-art in the relevant fields. This comparative analysis serves to establish the project's advancements and achievements, setting a benchmark against existing cutting-edge technologies and solutions.

Additionally, the document includes the positioning of IoT-NGIN's work on technological maps in the respective fields. This positioning exercise demonstrates how IoT-NGIN has effectively pushed the boundaries of the state-of-the-art in these domains. This step is crucial in laying the foundation for the development of clear value propositions and business plans within Tasks 8.2 and 8.3 of WP8.

Finally, this deliverable concludes the work undertaken in WP1, with a particular focus on Task 1.4: Continuous Technology Watch and Alignment on Next Generation IoT Advancements. The information and findings detailed in this report will serve as crucial input for WP8, where the project's technological outcomes will be leveraged for exploitation purposes. Specifically, this data will be instrumental in creating viable business plans for effectively utilizing and commercializing the innovative solutions developed as a part of the IoT-NGIN project.

In summary, this final deliverable of WP1 represents a significant milestone in the IoT-NGIN project. It not only provides a comprehensive understanding of the technological landscape in the IoT-NGIN sector but also establishes the project's progress in relation to the state-of-the-art in the relevant fields. The insights and analysis presented here will play a pivotal role in shaping the future direction of the project as it moves towards successful exploitation and the realization of its technological potential.

## 7 References

- [1] D.-I. p. European Commission, "EUSurvey," 31 July 2023. [Online]. Available: <https://ec.europa.eu/eusurvey/home/welcome>.
- [2] IoT-NGIN, "D1.3 - IoT meta-architecture alignment & continuous technology watch," H2020-957246 IoT-NGIN Deliverable Report, 2020.
- [3] K. Panetta, "3 Themes Surface in the 2021 Hype Cycle for Emerging Technologies," Gartner, [Online]. Available: <https://www.gartner.com/smarterwithgartner/3-themes-surface-in-the-2021-hype-cycle-for-emerging-technologies>. [Accessed 04 11 2022].
- [4] IoT-NGIN, "D2.2 - Enhancing IoT Underlying Technology," H2020-957246 IoT-NGIN Deliverable Report, 2022.
- [5] IoT-NGIN, "D2.3 - Enhanced IoT Underlying Technology (Final Version)," H2020-957246 IoT-NGIN Deliverable Report, 2023.
- [6] IoT-NGIN, "D2.1 - Enhancing IoT Underlying Technology," H2020-957246 IoT-NGIN Deliverable Report, 2021.
- [7] IoT-NGIN, "D3.3 - Enhanced IoT federated deep learning/reinforcement ML," H2020-957246 IoT-NGIN Deliverable Report, 2022.
- [8] IoT-NGIN, "D3.4 - ML models sharing and Transfer learning implementation," H2020-957246 IoT-NGIN Deliverable Report, 2023.
- [9] IoT-NGIN, "D4.3 - Enhancing IoT Tactile & Contextual Sensing/Actuating," H2020-957246 IoT-NGIN Deliverable Report, 2022.
- [10] IoT-NGIN, "D4.4 - Enhancing IoT Tactile & Contextual Sensing/Actuating (Final Version)," H2020-957246 IoT-NGIN Deliverable Report, 2023.
- [11] IoT-NGIN, "D5.2 - Enhancing IoT Cybersecurity (Update)," H2020-957246 IoT-NGIN Deliverable Report, 2022.
- [12] IoT-NGIN, "D5.3 - Enhancing IoT Data Privacy & Trust," H2020-957246 IoT-NGIN Deliverable Report, 2021.
- [13] IoT-NGIN, "D5.4 - Enhancing IoT Data Privacy & Trust (Update)," H2020-957246 IoT-NGIN Deliverable Report, 2022.
- [14] IoT-NGIN, "D5.5 - Enhanced IoT Cybersecurity & Data Privacy/Trust," H2020-957246 IoT-NGIN Deliverable Report, 2023.
- [15] IoT-NGIN, "D3.1 - Enhancing Deep learning/reinforcement learning," H2020-957246 IoT-NGIN Deliverable Report, 2021.

PENDING EC APPROVAL