

D.3.4 - Annual market and state of the art analysis in the context of IoT, AI and Cybersecurity: Third year.

Project Title: *Master of Science in Smart, Secure and Interconnected Systems*

Project Start Date: October 1st, 2022

Duration: 48 months

Call: DIGITAL-2021-SKILLS-01

Date of delivery: 31/03/2025

Topic: DIGITAL-2021-SKILLS-01-SPECIALISED

Dissemination Level: Public



Grant Agreement Number:	101083531
Project Title:	Master of Science in Smart, Secure and Interconnected Systems
Project Acronym:	MERIT
Document Number:	D3.4
Document Title:	Annual market and state of the art analysis in the context of IoT, AI and Cybersecurity: Third year
Version:	1.0
Delivery Date:	31/03/2025
Lead Beneficiary:	FBK
Editor(s):	Umberto Morelli (FBK)
Authors:	Umberto Morelli (FBK), Muhammad Imran (FBK)
Reviewers:	Egidijus Pilypas (Exacaster), Larisa Survilo (RTU), Agris Nikitenko (RTU), Cristian Maximiliano Rodriguez (UPC), Ilker Demirkol (UPC).
Keywords:	AI, Cybersecurity, IoT, Teaching topics and technologies, Research excellence, Industry needs
Status:	Final
Dissemination Level	Public
Project URL:	https://www.digitalmerit.eu/

Disclaimer: Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency (HADEA). Neither the European Union nor the HADEA can be held responsible for them.



Revision History

Rev. No.	Description	Author	Date
0.1	First draft	Umberto Morelli (FBK), Muhammed Imran (FBK), Federico Lenzi (FBK)	20.03.2025
0.2	Content review	Larisa Survilo (RTU), Agris Nikitenko (RTU), Egidijus Pilypas (Exacaster), Cristian Maximiliano Rodriguez (UPC)	26.03.2025
0.3	Content review	PMB (Ilker Demirkol - UPC)	28.03.2025
1.0	Final version	Integration of reviewers and PMB suggestions.	31.03.2025



Table of Contents

LIST OF TABLES.....	5
EXECUTIVE SUMMARY.....	6
1 INTRODUCTION.....	7
2 METHODOLOGY.....	8
2.1 Step 1 - Collect MERIT partner expertise.....	9
2.2 Step 2 - Collect MERIT universities vision for their students.	9
2.3 Step 3 - Identify data sources.	11
2.4 Step 4 - Data analysis.....	13
2.5 Step 5 - Investigate market needs.....	23
2.6 Step 6 - Cross data analysis and industry results	26
2.7 Step 7 - Merge data analysis and market needs with MERIT universities vision, and prioritise results.....	28
3 ROLES OF AI-CS AND AI-IOT	35
4 CONCLUSION.....	38
REFERENCES.....	39
APPENDIX A.....	41
APPENDIX B.....	42



List of Figures

Figure 1: Methodology to investigate current state-of-the-art and forecasted topics and competencies from both research and industry perspectives. The investigation includes the MERIT Universities desiderata.8	
Figure 2: Word cloud generated from MERIT universities programs learning outcome (left) and courses learning outcome (right).	10
Figure 3: Academic interest in the reported CS topics, technologies and application areas in the past five years using Scopus and specific queries and parameters (ref. to Appendix A).	29
Figure 4: Academic interest in the reported AI topics, technologies and application areas in the past five years using Scopus and specific queries and parameters (ref. to Appendix A).	30
Figure 5: Academic interest in the reported IoT topics, technologies and application areas in the past five years using Scopus and specific queries and parameters (ref. to Appendix A).	31
Figure 6: Framework for AI roles, common skills, and specific skills in age of industrial data space.	37

List of Tables

Table 1: MERIT Partners' areas of expertise.	9
Table 2: List of data sources, their domain and scope, and how it has been used in D3.4.	12
Table 3: CS topics, technologies and application areas obtained from data analysis.	16
Table 4: IoT topics, technologies and application areas obtained from data analysis.	20
Table 5: AI topics, technologies and application areas obtained from data analysis.	21
Table 6: Comparison of Step 4 results with past editions.	22
Table 7: Prioritised list of Cybersecurity topics, technologies and application areas for MERIT courses and related activities. "X ₁ " indicates those in line with Step 2 desiderata, "X ₂ " those deemed relevant from the Scopus database investigation.	28
Table 8: Prioritised list of Artificial Intelligence topics, technologies and application areas for MERIT courses and related activities. "X ₁ " indicates those in line with Step 2 desiderata, "X ₂ " those deemed relevant from the Scopus database investigation.	29
Table 9: Prioritised list of topics, technologies and application areas related to the Internet of Things for MERIT courses and related activities. "X ₁ " indicates those in line with Step 2 desiderata, "X ₂ " those deemed relevant from the Scopus database investigation.	31
Table 10: Step 7 results shared between D3.4 and D3.3.	32



Executive Summary

This document presents Deliverable 3.4 (D3.4) of the MERIT Work Package 3 (WP3): the third-year analysis of market needs, skill gaps, state-of-the-art and innovative approaches and technologies in the fields of Artificial Intelligence (AI), Cybersecurity (CS) and Internet of Things (IoT). It follows the methodology defined in Deliverable 3.1 (D3.1 – the first-year analysis) and revised in Deliverable 3.2 (D3.2 – the second) to identify new topics, skills, technologies and application areas to support MERIT activities, and to compare the results of past editions.

The document provides the following:

- The updated areas of expertise of MERIT consortium partners.
- The envisaged set of skills for students enrolled in MERIT master programs.
- The updated data sources identified by the MERIT consortium to investigate current and forecasted topics, technologies, application areas and skills in the AI, CS and IoT domains.
- A new set of data identified from research, statistics, reports and forecasts that are crucial to train the next generation of experts in the fields of AI, CS, and IoT and their interplays.
- The industry perspective over collected insights, regional (via three questionnaires online – for AI, CS and IoT) and more general (via industry reports) - a key enabler to make the study program operational.
- A carefully defined mapping that includes perspectives from research, industry and MERIT universities.
- A prioritised list of topics, technologies, application areas and skills that can be used to update and complement MERIT master programs and more general MERIT activities. As with D3.1/D3.2, the final list is also mapped to the skills, knowledge and occupations associated with the EU ESCO and e-CF frameworks, to highlight its applicability and impact in the European context.

The goals of the document are: (I) guide the design and upgrade of the MERIT master programmes (which correspond to MERIT WP5 and WP6, respectively) to support current and future skill needs, with graduates highly specialised in the most relevant AI, CS and IoT topics and technologies; (II) impact the society in line with the activities of the MERIT communication and dissemination strategy (part of MERIT WP2), and involve regional SMEs in the master programs to help filling potential regional skill gaps (highlighted/confirmed by them); (III) increase the expertise of consortium members from both the research and industry perspectives.



1 Introduction

By determining the most relevant present and upcoming topics and competencies in the Artificial Intelligence (AI), Cybersecurity (CS), and Internet of Things (IoT) domains, MERIT WP3 aims to shape the MERIT long-term strategy. The results have influenced the creation of MERIT master programs and related events, such as public outreach campaigns, hackathons, and upskilling campaigns. WP3 functions on three main levels:

- **Master Program Design** – Providing input on the relevant topics, skills, technologies and application areas to WP4 to initially structure MERIT master programs. This phase is currently completed.
- **Development of Program Materials** – Mapping expertise within the consortium to allocate responsibilities for the creation of course contents and activities related to identified topics, skills, and technologies (WP5).
- **Courses Administration** – Supporting the upskilling of educators and involved SME employees on the latest advancements in AI, CS, and IoT (WP6).

Additionally, WP3 collaborates with WP2 to enhance digital skills among its target audiences, ensuring effective communication and dissemination of key topics and competencies.

Objectives of WP3

- Strengthen the reputation of the consortium universities as leaders in AI, CS, and IoT domains, positioning them as go-to experts for digital competencies in academia and industry.
- Enhance teaching staff expertise through collaboration with diverse stakeholders, fostering knowledge exchange and synergies.
- Promote the growth of advanced digital skills in Europe by attracting students and professionals to AI, IoT, and CS master studies, enabling them to tackle the complexities of next-generation systems.

To achieve these objectives, **D3.4** builds upon the methodology established in the first-year analysis (**D3.1**) and iteratively updates it. The process identifies and prioritises key topics, skills, technologies and application areas and includes the perspectives of the research, industry and MERIT universities, ensuring continuous refinement of the MERIT master program and related initiatives. Each iteration compares findings with previous analyses to track progress and trends.

Organisation of the document

The document is organised as follows. Section [2](#) presents the seven-step methodology to identify the skills, topics and application areas, and its third application (also comparing the results with past editions). Section [3](#) provides the updated set of skills requested by the specialised job positions leveraging AI-CS or AI-IoT expertise. The deliverable concludes with Section [4](#), where a summary of the results and the link with other MERIT WPs are put forward. Two annexes report (i) the queries used to investigate the academic interest in the deliverable results leveraging the Scopus database (Annex [A](#)), and (ii) the script to verify how they align with the European skills and labour market via the European Skills, Competences, Qualifications and Occupations (ESCO) classification (Annex [B](#)).

2 Methodology

This Chapter describes the approach to investigate current and forecasted topics and competencies, comparing current results and insights with those of D3.2. Figure 1 summarises the methodology steps (indicated as flag numbers) performed by the different partners of the MERIT consortium.

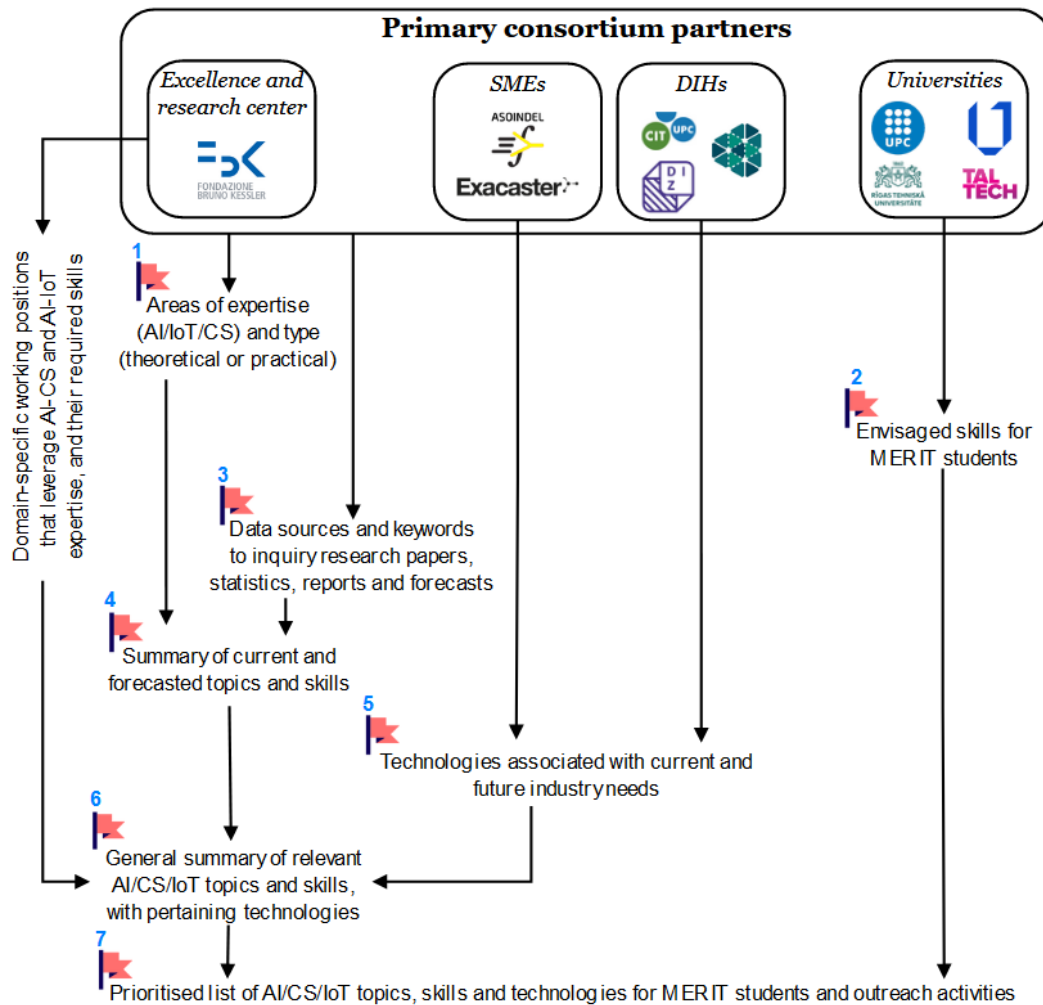


Figure 1: Methodology to investigate current state-of-the-art and forecasted topics and competencies from both research and industry perspectives. The investigation includes the MERIT Universities desiderata.

Figure 1 provides the MERIT consortium members: one Excellence and Research Centre (FBK), four Universities (UPC, Vilnius Tech, RTU, and TalTech), two SMEs (Exacaster and Asoindel), and three DIHs (CIT-UPC, DIZNE and SSMTTP). The methodology in the following takes advantage of FBK expertise to identify the domain-specific working positions (AI-CS and AI-IoT) and their required skills (put in Figure 1 on the left) and to summarise the output at each step. In addition, it distributes the responsibilities according to the different areas of expertise. In general, universities and FBK are asked to participate in state-of-the-art literature analysis, and SMEs and DIHs support the inquiry of market needs. The last step tries to integrate the MERIT Universities desiderata and prioritise identified topics, technologies, skills and application areas.



Approach

To understand the relevant set of topics and competencies for MERIT students (and a broader audience, following future MERIT outreach and upskilling activities), the consortium followed like D3.3 the methodology developed in deliverable D3.1 (which was inspired by the requirement elicitation process reported in [1]). In the following, we provide the seven steps and their new results, comparing them with the past editions.

2.1 Step 1 - Collect MERIT partner expertise.

Step 1 requires verifying each MERIT partner area of expertise, to focus contributions to the analysis and support the sharing of expertise and resources in the consortium. The goal is to create three groups (for AI, CS and IoT data sources and data - Step 3 and Step 4, respectively) according to the declared expertise.

Results:

Table 1 highlights how all three areas are covered from theoretical (**R**esearch and **T**eaching) and practical (**P**rototyping and **L**aboratories) perspectives. Therefore, the competence of the consortium members in investigating (and later administering) the necessary topics and set of skills. According to the reported expertise, Vilnius Tech and UPC was assigned to the AI group, RTU and Taltech the IoT group, and FBK participated in all groups and for the CS one.

Table 1: MERIT Partners' areas of expertise.

Partners	AI Expertise	Cybersecurity expertise	IoT Expertise
	Research, Teaching, Prototyping, hosting of Laboratories		
FBK	R, T, P	R, T, P	R, T, P, L
UPC	R, T, P, L	R, T, P, L	R, T, P, L
Vilnius tech	R, T, P	R, T, L	R, T, L
RTU	R, T, P, L	R, T, L	R, T, P, L
TalTech	R, T, P	R, T	R, T, P, L
Exacaster	R, P		
Asoindel	R, P		R, T, P, L
DIZNE	P	P	P
SSMTP	T	T, L	
CIT-UPC	R, P	R, P	R, P

After the increase in partner expertise observed in the last edition (8 new capabilities - see D3.3), the same expertise gets essentially confirmed in the consortium this year (although RTU no longer hosts laboratories and CIT-UPC also supports prototyping via its network of research centres - see *L* and *P* in Table 1, respectively). This is mainly due to (i) the change of focus from developing new capabilities and collaborations for master course creation to course delivery (leveraging those capabilities) and (ii) the core business of each partner (e.g., not providing services in the IoT domain). Most universities updated the existing infrastructure by adding modern computational resources and equipment for a broader range of experiments. For instance, virtual reality equipment is used to support student interaction rather than proposing software-only AI solutions.

2.2 Step 2 - Collect MERIT universities vision for their students.

Step 2 investigates the set of mandatory skills MERIT universities want their students to develop, to later prioritise identified topics/skills in the MERIT programme (see Step 7).



Results:

To obtain the envisaged set of topics and competencies for future MERIT students, D3.3 investigated the learning outcomes of the syllabi and of the courses of MERIT universities. Currently, MERIT master programs are operated by all consortium universities:

- *AI Engineering and Management of AI solutions* at Vilnius Tech.
- *Machine Learning and Cybersecurity for Internet-Connected Systems* at UPC.
- *Industrial Engineering and Management* at Taltech.
- *Management of Smart, Resilient, and Interconnected Systems*, since January 2025 at RTU.

Since the content of the study programs has not changed (yet), we provide the insights reported in D3.3 below. The data used to derive desiderata for Step 7 prioritisation is written in italics.

MERIT graduates from Vilnius Tech, Taltech, RTU, and UPC are expected to be proficient in various domains. Vilnius Tech programs focus on AI expertise, expecting graduates to *apply knowledge from informatics, project management, systems modelling, and data analysis* to the AI domain. They should be able to *document their work, implement solutions, communicate effectively in English, conduct research, work well in teams, exhibit critical thinking and lead when necessary, adhere to professional and ethical behaviour principles and understand the impact of proposed solutions*. Taltech program emphasises the *design and optimisation of integrated manufacturing systems, problem-solving* in manufacturing engineering and management, *waste reduction*, and understanding of *production planning and management*. Their students should develop technical systems to *solve economic problems and draft financial business plans, and lead when necessary*. RTU graduates are expected to be well-versed in the latest *advancements in AI, machine learning, data analytics, and IoT*. They should apply technology for *process efficiency*, make *technology-driven decisions*, be proficient in *strategy development and system design*, and understand the *legal and social aspects of system management*. UPC expects its graduates to describe *machine learning methods*, identify *challenges in machine learning*, understand *cybersecurity standards*, select appropriate *tools for IoT projects, evaluate AI, cybersecurity, and IoT solutions*, and apply *advanced computing knowledge*. They should also be able to *define complex AI problems, develop hardware or software systems, create innovative solutions, justify their solutions, communicate effectively in English, analyse security weaknesses, and apply solutions for security risks*. All universities emphasise the importance of *continuous learning, ethical standards, teamwork*, and the ability to *propose innovative and sustainable solutions*.

Figure 2 reports a word cloud based on the learning outcomes of the masters' syllabi and courses. Artificial intelligence plays a prominent role in both.

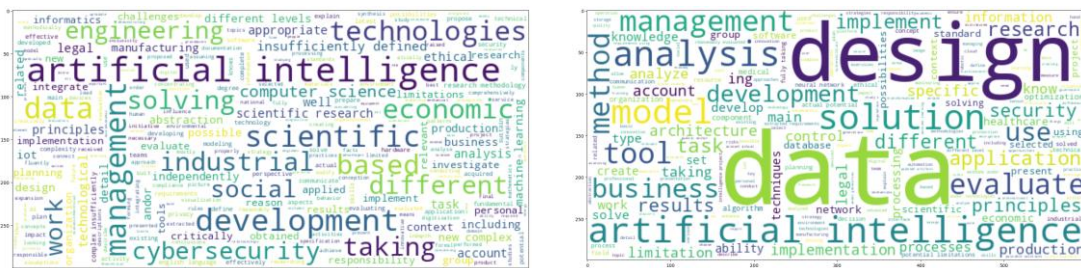


Figure 2: Word cloud generated from MERIT universities programs learning outcome (left) and courses learning outcome (right).



The first-year analysis (described in D3.1) emphasised the needs of the industry in which MERIT universities try to position themselves. However, the core competencies, such as fundamental knowledge, applied knowledge, communication skills, and the ability to learn/work efficiently and independently, all remain relevant and important in the syllabi as they form their foundation to achieve high-level job positions.

The second round of MERIT master students will enrol in September. We suggest that MERIT universities re-examine and upgrade learning outcomes (and their desiderata for MERIT master students), considering the results of this document.

2.3 Step 3 - Identify data sources.

Step 3 requires identifying (as a consortium) the set of data sources to gather the most relevant documents in the context of AI, CS and IoT.

Results:

Differently from the past editions (MERIT deliverables D3.1 and D3.3), where we reported all the data sources used to inquire the current and future needs in the target domains (AI, CS, IoT), we decided to list in Table [2](#) only data sources providing documents which have been analysed in Step 4. We therefore excluded the following sources as they did not provide up-to-date, relevant information (from January 2024 onwards), or we already collected enough data considering the scope (Global, EU, or Regional) or the category (Research or Statistics, Reports, Forecasts):

- BASE (Bielefeld Academic Search Engine).
- Ebsco.
- Google Scholar.
- Science Direct.
- Scopus.
- Web of Science / Web of Knowledge.
- Wiley Online Library.
- EC's AI Watch.
- EPoSS Association.
- Frost & Sullivan.
- Latvian Information and communications technology association.
- OECD.
- IEEE Robotics & Automation society.
- IEEE EAD.
- IEEE Innovation at Work.
- IoT Forum.

Table 2: List of data sources, their domain and scope, and how it has been used in D3.4.

Source with link	Scope	Domain	Used as a source of		
			Research or Statistics	Reports	Forecasts
ACM Digital Library	Global	AI,IoT	v		
Arxiv	Global	AI,IoT	v		
Association of Pacific Rim Universities	Global	AI	v	v	v
BCG	Global	AI		v	v
BMC Medical Research Methodology	Global	AI	v		
CLUSIT	Regional (IT)	CS		v	
ENISA	EU	CS	v	v	v
European Commission	EU	IoT		v	
Forbes	Global	CS			v
Gartner	Global	CS			v
IBM	Global	CS		v	v
IEEE Computer Society	Global	IoT			v
IEEE Internet of Things	Global	IoT	v	v	v
IEEE Xplore	Global	AI,IoT	v		
Initiative for applied artificial intelligence	Global	AI	v		
IoT Analytics	Global	IoT		v	
McKinsey & Company	Global	IoT,CS		v	v
MDPI	Global	AI,IoT	v		
Next Generation IoT	EU	IoT	v		
Researchgate	Global	AI,CS	v		v
SPD Technology	EU	IoT			v
Splunk	Global	CS		v	
Springer	Global	IoT	v		
Taylor & Francis Online	Global	IoT	v		
The REWIRE EU project	EU	CS	v		
US House of Representatives	Global	AI		v	
Verizone	Global	CS		v	
World Economic Forum	Global	AI,CS		v	

In line with past editions, we leveraged different regional sources and AI tools for data source discovery and Step 4 analysis. Differently, we decided that the discovery of data sources through keywords (e.g. using Google Dorks - see D3.3) could have limited the finding of data sources providing cutting-edge topics, technologies and application areas. Therefore, we did not update and report the list of keywords identified in D3.3.



2.4 Step 4 - Data analysis.

Step 4 analyses identified research papers, statistics, reports, and forecasts according to MERIT consortium expertise (ref. to Table 1).

Results:

Following the first-year approach, the MERIT consortium collected research, statistics, reports, and forecasts in three tables (one per domain – AI, CS and IoT) reporting the name, year (at least from 2024), link, scope (Regional, European or Global), and a summary of identified data.

General overview:

For a general perspective, the McKinsey & Company Technology Trends Outlook 2024 [2] highlights 15 technology trends (grouped in 5 categories), their potential economic value, talent gap and adoption rates, to help executives plan and navigate the fast-changing technology landscape. Considering the reported trends, Electrification and Renewables, Generative AI and Applied AI all report (in order) the highest value of interest¹-replacing Future of Mobility and Web3 in second and third place in last year's McKinsey analysis. Applied AI, Advanced Connectivity and the Future of Bioengineering, in line with past year analysis, rank (in order) among the top three innovation trends². Following are the highlighted talent gaps in order of talent deficit and ranked with **High**, **Medium**, and **Low** considering the talent to job demand ratio:

- DevOps, continuous integration and cloud computing (followed by software engineering, IT and Python) in the context of *Next-generation software development* - a trend with a talent demand of ~0.6:1 and maturity 3:5 in their investigation. Most requested job profiles: software engineer, software developer and data engineer.
- Machine learning, Artificial Intelligence and Python in *Applied AI* - talent demand between 0.2 and 0.3 (to 1); maturity 4:5. Most requested job profiles: data scientist, software engineer and data engineer.
- Sustainability, energy efficiency and construction (followed by waste management, manufacturing, regulatory compliance and hazardous materials) in *Climate technologies beyond electrification and renewable* - talent demand between 0.3 and 0.4 (to 1); maturity 2:5. Most requested job profiles: technician, project manager, general supervisor.
- Electric vehicles, automotive industry and IT (followed by vehicle fleet management and transportation management) in *Future of mobility* - talent demand between 0.2 and 0.4 (to 1); maturity 2:5. Most requested job profiles: software engineer, project manager, software developer.
- Renewable energy, photovoltaics and construction in *Electrification and renewable* - talent demand between 0.2 and 0.4 (to 1); maturity 3:5. Most requested job profiles: electrical engineer, project manager and mechanical engineer.
- Information technology, computer security and risk analysis (followed by stakeholder management, blockchain, identity theft and regulatory compliance) in *Digital trust and cybersecurity* (which replaces Web3 and trust architectures in the previous year's McKinsey analysis) - talent demand between 0.2 and 0.3 (to 1); maturity 3:5. Most requested job profiles: security analyst, software engineer and security engineer.
- Data centers, cloud computing and IT in *Cloud and edge computing* - talent demand between 0.2 and 0.3 (to 1); maturity 4:5. Most requested job profiles: software engineer, network engineer and solution architect.

¹ As reported, 0 to 1 score for news and searches, which are relative to the trends studied. The news score is based on a measure of news publications, and the search one is based on a measure of search engine queries.

² As reported, 0 to 1 score for patents and research, which are relative to the trends studied. The patent score is based on a measure of patent filings, and the research one is based on a measure of research publications.



- Kubernetes, Docker and Python (followed by cloud computing) in *Industrializing machine learning* - talent demand between 0.2 and 0.3 (to 1); maturity 3:5. Most requested job profiles: software engineer, software developer and data scientist.
- Telecommunications, IT and IoT (followed by electronics and construction) in *Advanced connectivity* - talent demand of less than 0.2 (to 1); maturity 4:5. Most requested job profiles: electronics technician, software engineer and network engineer.
- Virtual reality, augmented reality and mechanical engineering (followed by software engineering and product design) Immersive-reality technologies - talent demand of less than 0.1 (to 1); maturity 2:5. Most requested job profiles: electronics technician, software engineer and network engineer.
- Biology, biomedical engineering, molecular biology (followed by data analysis, pharmaceutical, biotechnology and gene therapy) in *Future of bioengineering* - talent demand near zero; maturity 2:5. Most requested job profiles: electronics technician, software engineer and network engineer.
- Aerospace engineering, manufacturing and system engineering (followed by Python, physics, space exploration and remote sensing) in *Future of space technologies* - talent demand near zero (~0.05 to 1); maturity 1:5. Most requested job profiles: electronics technician, software engineer and network engineer.
- Artificial Intelligence, Machine learning and Python in *Generative AI* - talent demand between 0.3 and 0.4 (to 1); maturity 4:5. Most requested job profiles: data scientist, software engineer and data engineer.
- Automation, mechatronics and manufacturing (followed by AI, Python, software engineering and data analysis) in *Future of robotics* - talent demand near zero (between 0.02 and 0.04 to 1); maturity 2:5. Most requested job profiles: software developer, data scientist and software engineer.
- Quantum computing, physics and AI (followed by Python, cloud computing, algorithms and ML) in *Quantum technologies* - talent demand near zero (0.01:1); maturity 1:5. Most requested job profiles: software engineer, scientist and data scientist.

Cybersecurity overview:

The cybersecurity ecosystem is facing unprecedented challenges, with nation-state actors, cybercriminals, and AI-powered threats escalating in complexity. The cost of cybercrime is projected to reach \$10.5 trillion annually by 2025, up from \$3 trillion in 2015 [3], reflecting a dramatic increase in attack frequency and sophistication. 9 significant incidents per day globally, mainly targeting healthcare, are indicated by CLUSIT in its report [4]³. Organisations must not only defend against cyberattacks but also ensure resilience through proactive strategies, regulatory compliance, and cross-sector collaborations. Drawing from a wide range of sources - including reports from ENISA, Clusit, WEF, Gartner, IBM, McKinsey, and different academic research – we report below some of the most interesting insights.

The Microsoft Digital Defense Report 2024 [5] highlights that nation-state actors are increasingly engaging in cyber warfare, espionage, and influence operations. These groups exploit vulnerabilities in critical infrastructure, with an estimated 600 million identity attacks occurring daily. The number of state-sponsored cyberattacks has increased by 40% in the past year, targeting governments, financial institutions, and technology companies. Cyberattacks linked to espionage have resulted in the theft of over 200 terabytes of sensitive data globally. Microsoft and Google have identified over 1,500 active nation-state threat groups operating worldwide, with China, Russia, Iran, and North Korea leading in cyber aggression.

³ Italy accounted for 7.6% of worldwide incidents, illustrating regional vulnerabilities. Manufacturing and healthcare are among the most affected sectors.



AI and machine learning are transforming both cyber defence and cyber-attacks [6] [7] [8] [9] [10] [11] [8]. According to the World Economic Forum's Global Cybersecurity Outlook 2025 [12], 66% of organisations expect AI to significantly impact cybersecurity in the next year, yet only 37% have processes to assess AI security risks before deployment. AI-driven threat detection, predictive analytics, and automated incident response are becoming essential tools for cybersecurity resilience, allowing savings for \$2.2 million [9] by reducing detection and containment times. Additionally, AI-generated phishing attacks have increased by 125%, making traditional security defences less effective. AI-driven SOC (Security Operations Centres) are reducing response times by 95%, helping organisations mitigate threats in real time. ENISA's Threat Landscape 2024 [13] report emphasises that ransomware remains a prime target, while malware - including advanced forms such as FraudGPT - exploits vulnerabilities in both cloud services and enterprise networks. Cybercrime constitutes 88% of global attacks, with malware (especially ransomware) accounting for 34% of attack methods.

Ransomware remains a top concern, with a 2.75x increase in human-operated ransomware attacks. Supply chain security has become a critical priority [14], as interconnected ecosystems provide multiple attack vectors for cybercriminals. In 2023 alone, ransomware groups extorted over \$1.5 billion from businesses, with an average ransom demand of \$5.3 million per incident. More than 60% of all ransomware attacks now target supply chains, with attackers exploiting vulnerabilities in third-party vendors and software providers. The time to detect and contain a ransomware attack has also increased to an average of 23 days, significantly impacting business continuity and financial stability.

Cyber regulations are expanding globally, creating compliance complexities. The EU Cyber Resilience Act and U.S. cybersecurity mandates are reshaping corporate security strategies. However, 76% of CISOs report that fragmented regulations across jurisdictions create significant compliance challenges [15]. In 2024, over 90 new cybersecurity regulations were introduced worldwide, requiring businesses to allocate more resources to compliance efforts. Non-compliance penalties have increased by 65%, with organisations facing potential fines of up to \$20 million or 4% of their global annual revenue. The financial sector has seen the most stringent regulatory measures, with 85% of institutions investing in enhanced compliance frameworks to meet new mandates.

With quantum computing on the horizon, organisations are investing in post-quantum cryptography to prevent the potential decryption of encrypted data by future quantum systems. The National Institute of Standards and Technology (NIST) has been actively developing quantum-resistant algorithms, with global investments in quantum cryptography projected to reach \$3 billion by 2027. Over 60% of enterprises are expected to start transitioning to quantum-secure encryption protocols by 2030 to mitigate potential risks from quantum computing advancements.

Organisations are also exploring AI-based security tools to gain a competitive edge against evolving cyber threats, e.g., via real-time monitoring, anomaly detection, and automated remediation. AI-powered cybersecurity solutions have reduced false positives by 85%, improving detection accuracy. Furthermore, security teams using AI-driven analytics have reported a 70% increase in their ability to detect previously unknown attack patterns. The AI cybersecurity market is expected to grow at a CAGR of 23.3%, reaching \$133.8 billion by 2030.

Zero Trust is becoming the gold standard for security frameworks [14], ensuring that no entity is implicitly trusted. Organisations are integrating Zero Trust principles into their cybersecurity strategies to mitigate insider threats and external attacks. Adoption of Zero Trust frameworks has increased by 45% year-over-year, with 90% of enterprises planning to implement Zero Trust policies by 2026 [16]. Companies that have fully adopted



Zero Trust architectures report a 50% reduction in successful cyberattacks and an average savings of \$1.76 million per data breach incident.

Initiatives like the AI Cyber Challenge and collaborative threat intelligence sharing are essential for mitigating cyber risks at scale. Government and private sector partnerships have increased by 60%, leading to a 40% improvement in real-time threat intelligence sharing. Major tech firms, including Microsoft, Google, and AWS, have pledged a combined investment of \$30 billion over the next five years to strengthen cybersecurity infrastructure. Additionally, public-private collaborations have been instrumental in dismantling over 300 cybercriminal networks in the past two years.

Finally, job advertisements in the CS field [17] indicate a strong need for collaboration and communication skills (83.91% of advertisements) and Problem Solving and Critical Thinking (56.73%).

Table 3 provides the result of Step 4 data analysis for the CS domain: 20 reports, 11 academic work, 11 forecasts and 1 statistic, from 2024 and 2025, with Italian, EU and Global scope.

Table 3: CS topics, technologies and application areas obtained from data analysis.

CS topics and technologies	CS application areas
<ul style="list-style-type: none"> • Analysis of ransomware. • Analysis of malware. • Human-factor in security. • Supply chain attacks. • Zero Trust. • Incident Response. • Cyber Threat Intelligence. • Vulnerability management. • AI/ML in cybersecurity. • Security of cloud-edge continuum. • Cyberwarfare and Geopolitical Risks. • Advanced Persistent Threats (APTs). • Data Protection, pseudonymisation and privacy (regulatory compliance, engineering). • Disinformation and Influence Operations. • Generative AI Risks and Applications (deepfakes, fraud tools). • AI-Based tools. • Quantum computing. • Blockchain. • Incident Detection and response systems. • Privacy-Enhancing Technologies (PETs). • Cybersecurity automation. • Threat Intelligence Platforms. • Cyber Risk Assessment and Management Tools. • Identity Protection and Access Management. • Endpoint Security Solutions. • AI Honeypots and Deception Strategies. 	<ul style="list-style-type: none"> • Critical Infrastructure Protection. • Healthcare. • Financial services. • Supply chain Security. • Education and Training. • Regulatory Compliance. • Cybersecurity of manufacturing and industrial sectors (supply chain resilience).



IoT overview:

Market Trends and Growth Projections

The IoT market demonstrates robust growth trajectories, with the number of connected devices projected to increase from 40 billion in 2023 to 49 billion by 2026, representing a 7% annual growth rate [18]. More aggressive estimates suggest up to 75 billion devices globally by 2025 [19]. Enterprise spending on IoT increased by 10% year-over-year, reaching approximately \$298 billion [20], with the overall IoT market expected to grow at a compound annual growth rate (CAGR) of 17% until 2030 [21]. The market value is anticipated to double from \$300 billion in 2021 to \$600 billion by 2026 [22], demonstrating resilience despite economic fluctuations and geopolitical tensions.

The Artificial Intelligence of Things (AIoT), a convergence of AI and IoT, is creating a separate market projected to reach \$253.86 billion by 2030 [19]. Despite this growth, there has been a shift in corporate focus, with AI increasingly overshadowing IoT in executive communications and earnings calls. However, IoT remains among the top three corporate technology priorities for investment.

Key Technologies and Innovations

- **Edge Computing and Data Processing.** Edge computing has emerged as a pivotal technology that enables data processing closer to the source and reduces latency and bandwidth costs. This approach supports real-time operations and enhances data security and privacy. The industry is witnessing a shift from traditional cloud computing to a cloud-edge continuum, where processing is distributed between cloud and edge devices, optimising resource utilisation and efficiency.

Multi-access Edge Computing (MEC) improves data processing efficiency, while fog computing serves as an intermediate layer particularly effective for real-time applications like traffic control and public safety. These technologies help address data growth challenges and the diversity of data types generated by IoT devices.

- **Artificial Intelligence and Data Analytics.** AI integration is recognised as a significant tailwind for the IoT market, enhancing data processing and decision-making capabilities. Applications include:
 - Predictive maintenance in industrial settings.
 - Enhanced diagnostics in healthcare.
 - Optimisation of production processes through generative AI.
 - Cybersecurity improvements using Large Language Models (LLMs) and multimodal generative models.

Developing cognitive computing and smart IoT platforms facilitates industrial collaboration and more intelligent automated systems. Data fabric solutions are emerging as transformative approaches to managing and integrating data across various platforms and environments.

- **Connectivity and Communication.** Various communication technologies are crucial for IoT applications:
 - 5G networks for high-bandwidth, low-latency applications.
 - Narrowband IoT (NB-IoT) gaining traction due to cost-effectiveness and support for numerous devices.
 - LoRaWAN for wide-area coverage with low power consumption.
 - Wi-Fi, ZigBee, and Z-Wave for specific use cases and environments.



These technologies enable the necessary connectivity infrastructure for IoT ecosystems, supporting the growing number of interconnected devices and data exchange.

Application Areas

- **Industrial IoT and Manufacturing.** The industrial sector shows a divergence in growth patterns, with software vendors reporting optimism and over 12% growth in the industrial software market, while some hardware segments have faced declines [20]. IoT in manufacturing facilitates:
 - Implementation of cyber-physical systems enhancing operational efficiency.
 - Predictive maintenance, therefore reducing downtime.
 - Automation and smart manufacturing practices, reducing costs.
 - IT/OT convergence strategies integrating information technology with operational technology.
- **Smart Cities and Urban Infrastructure.** IoT technologies are integral to developing smart infrastructure and improving urban living through:
 - Traffic management and smart transportation systems.
 - Waste management optimization.
 - Energy efficiency improvements.
 - Environmental monitoring.
 - Public safety and crowd monitoring systems.

These applications leverage real-time data collection and analysis to enhance service delivery and reduce environmental impact.

- **Healthcare.** IoT devices are transforming patient care through:
 - Remote health monitoring and management.
 - Telemedicine applications.
 - Disease diagnosis using data from wearable devices.
 - Automation of healthcare processes.
 - Enhanced patient outcomes through continuous monitoring.
- **Agriculture and Energy.** In agriculture, IoT enables precision farming techniques that enhance crop management and resource efficiency.

For energy management, IoT applications support the transition to smart grids, optimising consumption and promoting sustainability in line with the European Green Deal and UN Sustainable Development Goals.

Challenges and Opportunities

- **Security and Privacy Concerns.** As IoT ecosystems expand, security and privacy concerns remain paramount. Challenges include:
 - Protection of sensitive data against evolving cyber threats.



- Need for robust regulatory frameworks.
- Balancing security with low latency requirements.
- Ensuring user control over personal data and privacy settings.
- **Interoperability and Standardisation.** The need for platform interoperability and standardisation becomes critical for seamless integration across devices and applications. The diversity of IoT devices and technologies leads to significant interoperability issues, which must be addressed through:
 - Development of common protocols and standards.
 - Open ecosystems and collaborative efforts among industry players.
 - Standardised frameworks to facilitate seamless integration.
- **Human-Centred Design and Autonomy.** There is a growing emphasis on designing IoT systems that prioritise human autonomy and user control over personal data. Key considerations include:
 - Human-centred design principles ensuring users can influence automated systems.
 - Personalised privacy settings.
 - Inclusive approaches considering diverse stakeholder perspectives.
 - Empowering users to actively manage their data and privacy.
- **Research and Funding Initiatives.** Significant funding and research initiatives are driving innovation in the IoT sector:
 - The European Commission is investing approximately €150 million in Horizon Europe projects focused on meta operating systems, decentralized intelligence, and edge computing (2022-2025) [18].
 - Research priorities include enhancing platform interoperability, cybersecurity, and technology integration.
 - Development of specialised tools and benchmarks for emerging technologies like Generative AI models tailored to IoT scenarios.

Future Directions

The IoT landscape is evolving toward:

- Web 4.0 and spatial computing, moving from traditional cloud computing to advanced digital twin technologies.
- Establishment of common European data spaces and EU-US collaborative research ecosystems
- Greater emphasis on sustainability and energy-efficient devices.
- Development of open IoT platforms enhancing innovation and market access for SMEs and startups.
- Integration of emerging technologies such as Brain-Computer Interfaces (BCIs) and autonomous systems.

This comprehensive overview highlights the dynamic nature of the IoT ecosystem, characterised by technological innovation, expanding application domains, and evolving market demands. The convergence of IoT with other technologies, particularly AI, edge computing, and advanced connectivity solutions, is creating new opportunities while also presenting challenges related to security, interoperability, and human-centred design that must be addressed to realise the full potential of IoT.



Table 4 provides the result of Step 4 data analysis for the IoT domain (9 research papers, 4 reports and 2 forecasts - one from 2022, five from 2023 and the rest from 2024 and 2025 - with EU and Global scope).

Table 4: IoT topics, technologies and application areas obtained from data analysis.

IoT Topics and technologies	IoT Application areas
<ul style="list-style-type: none"> • Building automation in IoT. • Applied AI for IoT solutions. • IoT autonomous Systems. • Cellular IoT (2G/3G/4G/5G). • IoT data ecosystems and IoT data spaces. • Digital Twins. • Edge Computing. • Intelligent Sensors. • IoT-based Analytics. • IoT Platforms. • Satellite IoT. • Wearables. 	<ul style="list-style-type: none"> • IoT in agriculture. • IoT for autonomous vehicles. • IoT solutions for climate and sustainability. • IoT in the energy domain. • IoT for the environment and green transition. • IoT in healthcare. • IoT solutions for logistics and supply chain. • IoT manufacturing solutions. • IoT solutions for mobility and transportation. • IoT solutions for public safety. • IoT solutions for robotics and the metaverse.

AI overview:

Artificial Intelligence (AI) is reshaping industries, driving innovation in education, cybersecurity, business automation, and industrial operations. This paragraph explores AI's applications, challenges, and future trends, emphasising the need for responsible governance and workforce adaptation.

- **AI in Higher Education:** AI enhances learning experiences, administrative efficiency, and student engagement through platforms like TECgpt and Cogniti. However, ethical concerns such as plagiarism, bias, and inequitable access require governance frameworks for responsible AI integration.
- **AI and Cybersecurity:** AI serves as both a defensive tool and a threat. While it strengthens threat detection, automated incident response, and SOC operations, cybercriminals exploit AI for deepfake impersonation and automated attacks. Securing AI itself through explainable AI (XAI) and adversarial defences is crucial.
- **Generative AI & Business Automation:** AI-driven automation is revolutionising software development, testing, and workflow optimisation. The shift from Robotic Process Automation (RPA) to Agentic Process Automation (APA) enables more adaptive, goal-driven AI applications. Challenges include bias, trustworthiness, and adversarial vulnerabilities.
- **AI in IoT and Industry:** AI is advancing smart manufacturing, predictive maintenance, and industrial security through:
 - Edge AI for real-time decision-making.
 - Digital twins for process optimisation.
 - Federated learning for privacy-preserving AI in IoT. However, data privacy and security risks remain a challenge.



• **AI Adoption & Workforce Challenges**

- The document highlights that Nordic enterprises are lagging in AI adoption, potentially affecting economic growth. AI integration could contribute €55 billion annually to the region’s GDP.
- However, 51% of employers report a skills gap in AI literacy, emphasising the need for AI-focused workforce training and educational reforms.

• **Key AI Technologies Driving Innovation**

The report highlights breakthrough AI technologies:

- Machine Learning & Deep Learning – Applied across multiple industries.
- Generative AI & LLMs – Transforming content creation and cybersecurity.
- Quantum AI – Enhancing cryptography and security.
- Edge AI – Powering real-time industrial automation.
- Digital Twins – Simulating real-world systems for optimisation.
- Federated Learning – Ensuring data privacy in AI applications.

• **Governance, Ethics & Future Challenges**

- The rapid adoption of AI raises concerns about bias, transparency, and accountability. The report stresses the importance of:
 - Strong AI governance frameworks to ensure ethical deployment.
 - Compliance with emerging regulations (e.g., AI Act, GDPR).
 - AI literacy programs and workforce reskilling to bridge the skills gap.

AI presents vast opportunities for innovation and automation, but its potential must be balanced with governance, ethical considerations, and workforce preparedness. Strategic AI adoption will be key to ensuring long-term economic growth and security.

Table 5 provides the result of Step 4 data analysis for the AI domain (6 research papers and 7 reports – half providing also statistics and forecasts, from 2024 and 2025, with EU and Global scope).

Table 5: AI topics, technologies and application areas obtained from data analysis.

AI topics and technologies	AI application areas
<ul style="list-style-type: none"> • Generative AI & Business Automation. • AI Adoption & Workforce Challenges. • Governance, Ethics & Future Challenges. • Machine Learning & Deep Learning. • Generative AI & Large Language Models (LLMs). • Quantum AI. • Edge AI. • Digital Twins. • Federated Learning. 	<ul style="list-style-type: none"> • AI in Higher Education (Learning Experiences, Administrative Efficiency, Student Engagement). • AI and Cybersecurity (Threat Detection, Automated Incident Response, SOC Operations). • AI in IoT and Industry (Smart Manufacturing, Predictive Maintenance, Industrial Security). • Business Automation (Software Development, Testing, Workflow Optimisation) • Workforce Development (AI Literacy, Workforce Reskilling, Educational Reforms). • Governance & Compliance (AI Ethics, Regulatory Compliance, Explainable AI).



Comparison of results and insights to past editions (D3.3 and D3.1).

The comparison in Table 6 provides an overview of topic alignment and evolution in AI, CS and IoT across the three deliverables (D3.4, D3.3 and D3.1). It offers a detailed breakdown combining numerical insights and key observations.

Table 6: Comparison of Step 4 results with past editions.

	Total number	Compared to D3.3		Compared to D3.1	
		Shared results	Unique results (in D3.4)	Shared results	Unique results (in D3.4)
AI	D3.4: 25 D3.3: 19 D3.1: 14	Explainable AI (XAI), Adversarial AI, AI-driven cybersecurity, Digital twins, Federated learning, Reinforcement learning, AI-powered analytics, NLP (Natural Language Processing), AI in decision-making, AI for robotics.	AI in edge computing, AI risk assessment, ethical AI governance and AI for smart manufacturing.	Machine learning applications, Reinforcement learning, AI-enabled decision-making, Robotics, NLP (Natural Language Processing), AI-powered analytics, AI for cybersecurity.	AI ethics, multimodal AI systems, AI-powered automation in critical infrastructure (e.g., healthcare, energy, IoT).
CS	D3.4: 35 D3.3: 30 D3.1: 28	Zero Trust security, Authentication protocols, Malware analysis, Adversarial attacks, AI-driven threat detection, Cryptographic methods, Cloud security, Risk-based access control, Identity verification, Cyber risk management.	Cybersecurity in manufacturing, automated security operations, cloud-based security solutions, cybersecurity for critical infrastructure, and cybersecurity in healthcare.	Cyber risk management, Encryption methods, Identity verification techniques, Access control, Network security, AI-driven cybersecurity, Security frameworks, Incident response strategies	Cybersecurity for industrial IoT, AI-enhanced threat intelligence, cybersecurity policy advancements, and regulatory frameworks.
IoT	D3.4: 26 D3.3: 22 D3.1: 18	IoT security, Smart city technologies, Industrial IoT applications, Edge computing, Device management, Real-time monitoring, IoT data processing, Cloud-IoT integration, Network protocols (e.g., MQTT), IoT-based predictive maintenance, Secure IoT authentication and Data privacy in IoT	AI-driven anomaly detection for IoT security (new approach to secure IoT networks).	Real-time monitoring, connected devices, Cloud-IoT integration, Network protocols (e.g., MQTT), IoT security, Smart sensors, IoT-enabled industrial automation, Energy-efficient IoT systems and Wireless communication in IoT.	AI-driven anomaly detection for IoT security (enhancing device security and threat mitigation).

Key Takeaways:

The D3.4 analysis reveals key developments in Cybersecurity, Artificial Intelligence (AI), and the Internet of Things (IoT), highlighting shifts in focus and emerging trends. The report underscores the growing integration of AI-driven solutions across these domains, reflecting the evolving landscape of technology and security.

Cybersecurity:

In the domain of cybersecurity, current analysis places a stronger emphasis on AI-driven cybersecurity, automated security operations, and cybersecurity for critical infrastructure, marking a shift towards more intelligent and domain-specific security solutions. AI-enhanced threat intelligence and automated security operations have gained prominence, expanding beyond traditional cybersecurity methods. There is a notable increase in



industry-specific concerns, particularly in securing industrial IoT, manufacturing, healthcare, and energy sectors. Additionally, regulatory frameworks and compliance management have been emphasised to address evolving cyber risks, reflecting the increasing importance of cybersecurity policies in the digital era.

Artificial Intelligence:

In the AI domain, current analysis highlights advancements in AI ethics, AI-powered automation, and multi-modal AI systems, indicating a shift toward more specialised and industry-focused applications. Ethical AI governance and AI risk assessment have become critical areas, ensuring AI systems remain transparent, unbiased, and accountable. The integration of AI in edge computing, smart manufacturing, and AI-driven cybersecurity demonstrates the growing emphasis on applied AI solutions. Moreover, the expansion of multi-modal AI systems and AI-powered automation in critical infrastructure such as healthcare, energy, and IoT signifies an increasing reliance on AI for decision-making across multiple domains.

Internet of Things (IoT):

D3.4 maintains a stable focus on IoT security, real-time monitoring, and cloud integration, while introducing AI-driven anomaly detection as a key enhancement for IoT security. AI-driven security measures have gained importance in mitigating threats and ensuring device authentication. IoT applications continue to be widely adopted across smart cities, healthcare, manufacturing, and energy, with AI playing an increasingly vital role in predictive analytics and security improvements. The growing intersection of AI and IoT highlights the industry's shift toward more intelligent and automated IoT security frameworks.

2.5 Step 5 - Investigate market needs.

Step 5 is implemented by requesting partner SMEs to highlight their needs and, together with DIHs, inquire about regional market needs by administering a questionnaire in their network. In the following results, we provide the number of organisations participating in the questionnaire, their field of operation, and their response on the current or future use of specific technologies or topics/skills in specific application areas. Data is finally compared with the past editions of the methodology.

Results:

Cybersecurity questionnaires discussion:

15 organisations integrating cybersecurity measures and technologies responded to the Cybersecurity questionnaire: seven operating in Information Technology and Services (e.g., consulting), one in software and automation, and others instead offering more general services (e.g., manufacturing and education).

The results we want to highlight are:

- 9/15 currently leverages (A) cybersecurity mechanisms that evaluate the *human-factor* (e.g., protections against social engineering and phishing) and (B) measures to foster *data protection, pseudonymisation and privacy* (e.g., to comply with regulations); (A) will be integrated by 2 organisations within one year, (B) by 1 organisation within one year and another between one and two years. 9 organisations also indicate that regulatory compliance is a skill leveraged as part of their daily operation, while 9 do not consider Healthcare Security similarly.
- 8/15 currently support (C) Zero Trust and (D) Vulnerability Management; (C) 2 organisations within one year and one between one and two years; (D) 1 organisation within one year. 8 organisations also adopt Cyber Risk Assessment and Management Tools, while 2 organisations plan to do it within two years.
- 7/15 adopt Incident Response mechanisms, while 2 plan to do it within one year. 7/15 also integrate a (E) Zero Trust Architecture, a (F) Threat Intelligence Platforms, (G) specific Identity Management and Access



Control solutions (e.g., MFA or risk-based authentication) and (H) Endpoint security solutions; (E) 3 organisations between one and two years, (F)(G)(H) 1 organisation, respectively, between one and two years.

- 1/15 operates in the quantum computing domain, while 7 do not (and 2 do not know).

In the current edition, all respondents use or will use the queried cybersecurity expertise, topic or technologies. No additional cybersecurity topics, technologies or application areas were indicated.

16 (upon 23) cybersecurity topics and expertise from D3.4 questionnaires can be directly linked with D3.3 ones: Critical Infrastructure Protection; Analysis of Ransomware; Analysis of Malware; Human-factor in Security (e.g., Social Engineering and Phishing); Supply Chain Attacks; Incident Response; Cyber Threat Intelligence; Vulnerability Management; AI/ML in Cybersecurity; Advanced Persistent Threats (APTs); Disinformation and Influence Operations; Generative AI Risks and Applications (deepfakes, fraud tools); Healthcare Security; Financial Services Protection; Supply Chain Security; Cybersecurity of Manufacturing and Industrial Sectors (supply chain resilience). Differently, organisations now report an interest in *data protection, pseudonymisation and privacy, Regulatory Compliance and Education and Training*.

9 (upon 12) cybersecurity technologies can be directly linked: AI-Based Tools; Blockchain; Incident Detection and Response Systems; Zero-Trust Architecture; Privacy-Enhancing Technologies (PETs); Cybersecurity Automation; Threat Intelligence Platforms; Identity Protection and Access Management; Endpoint Security Solutions. Differently, organisations now report an interest in *Cyber Risk Assessment and Management Tools*.

AI questionnaires discussion:

25 organisations operating in AI-related domains responded to the AI questionnaire: five operating in Information Technology and Services (e.g., software development and manufacturing), three in software and automation, two focused on AI solution development and one AI R&D; the rest dedicated to data analytics and more general services (e.g., career development and education).

The results we want to highlight are:

- More than half of the respondents do not leverage the following expertise: AI-driven Security Operations Center (SOC); AI for IoT Security; Quantum AI; Digital Twin (i.e., Simulating and optimising IoT system security with AI-powered digital replicas); AI in Autonomous Driving (i.e., AI's role in vehicle navigation, collision avoidance, and safety); AI for Environmental Sustainability (i.e., AI applications for reducing waste, energy usage, and climate change mitigation) and AI in Healthcare (e.g., AI tools for diagnostics, treatment planning, and patient care optimisation).
- AI in Retail (i.e., Personalised recommendations, customer behaviour analysis, and inventory management), AI in Smart Manufacturing (i.e., tools for automated quality control, predictive maintenance, and process optimisation) and Generative AI Technologies for Cybersecurity are used currently or in future by almost half of participants.

All respondents use or will use the queried AI expertise, topic or technologies. Respondents also suggested to integrate:

- AI as an engineering tool for project development.
- AI tools for manufacturing planning optimisation tasks.
- Adoption of reinforced learning.
- (more general) Generative AI and LLMs (e.g., chatbots, information search, automation, AI agents).
- Virtual reality.
- Agentic AI applications.



- Technical and legal aspects of data and ML/AI model sharing.
- Data and ML/AI model lifecycle management.

5 (upon 18) AI-related topics and expertise from D3.4 questionnaires can be directly linked with D3.3 ones: AI in Smart Manufacturing, Autonomous Driving and Healthcare; AI Ethics and Governance and AI for Environmental Sustainability.

14 (upon 19) AI-related technologies can be directly linked: AI in Retail; AI in Financial Systems; AI in Healthcare; AI for Environmental Sustainability; AI in Autonomous Driving; AI in Smart Manufacturing; Multi-Agent Systems for Cybersecurity; Training for AI-Cybersecurity Skills; AI-Powered Penetration Testing; AI-Enhanced Vulnerability Scanning; Federated Learning for IoT; AI-Driven SOC Automation; Generative AI Technologies; Machine Learning for Cybersecurity.

IoT questionnaires discussion:

13 organisations operating in IoT-related domains responded to the IoT questionnaire: four operating in Information Technology and Services (e.g., energy operator), one in software and automation; others instead offering more general services (e.g., robotics and education).

The results we want to highlight are:

- More than half of participants indicated that all IoT applications (except IoT for *Public Safety* – e.g., coordinated emergency alerts) are currently deployed in their region or are intended to be deployed within one year (excluded IoT for *Autonomous Vehicles*, *Climate and Sustainability* and *Public Safety*). One respondent highlighted the use of IoT for military.
- More than half indicated the current deployment of the following technologies: *Applied AI* (in the context of IoT), *Cellular IoT (2G/3G/4G/5G)*, *Digital Twins*, *Edge Computing*, *Intelligent Sensors*, *IoT-based Analytics*, *IoT Platforms*, *Smart IoT Platforms* and *Wearables*.

In the current edition, all IoT applications and technologies are used in respondents' regions.

5 (upon 13) IoT application areas from D3.4 questionnaires can be directly linked with D3.3 ones: *Smart Agriculture*; *Healthcare*; *Smart Industry*; *Smart Transportation*; *Smart Environment*.

8 (upon 12) IoT technologies can be directly linked with D3.3 ones: *Cellular IoT (2G/3G/4G/5G)*; *Data Ecosystems or Data Spaces*; *Digital Twins*; *Intelligent Sensors*; *IoT Platforms*; *IoT-based Analytics*; *Smart IoT Platforms*; *Edge Computing*.

In line with the approach followed in D3.1, we sought a broader overview of industry needs through three reports by Frost & Sullivan (considering their large experience in market analysis) [23] [24] [25]. Their analysis outlines the following future industry skill needs:

- **Cybersecurity:** There will be a growing demand for skills in cloud computing security, penetration testing, threat intelligence analysis, and forensics. Additionally, governance, risk management, and compliance (GRC) skills will become increasingly important.
- **IoT:** As IoT continues to expand, skills related to monitoring and managing IoT devices will be critical, particularly in the context of security and data management.
- **AI:** The need for professionals with expertise in AI and machine learning will rise, particularly those who can integrate these technologies into existing business processes and enhance operational efficiency. The growing intersection of AI and IoT highlights the industry's shift toward more intelligent and automated IoT security frameworks.



2.6 Step 6 - Cross data analysis and industry results

Step 6 aims to generate a summary of required AI, CS and IoT technologies and skills/topics by considering both the data analysis (Step 4) and industry questionnaires (Step 5).

Results:

The following set provides the **CS** topics, technologies and application areas currently leveraged by at least half of the organisations participating in CS questionnaires, joined with those indicated by Frost & Sullivan:

- Human factors in cybersecurity: e.g., training to protect against social engineering and phishing.
- Zero Trust framework: security measures at the different layers and ways to support them.
- Practical incident response: e.g., using a well-established Extended Detection and Response (XDR) solution.
- Data protection and privacy (e.g., pseudonymisation but also including the privacy- and security-aware use of AI tools).
- Cyber Threat Intelligence: particularly, the types of intelligence and how to process and present them.
- Cyber risk assessment, governance and management tools.
- Identity Protection (e.g., multi-factor or risk-based authentication) and Access Management (e.g., A privileged access workstation - PAW).
- Endpoint Security Solutions: endpoint detection and response (EDR).
- Regulatory compliance (e.g., towards NIS2) and support of well-known best practices (e.g., from OWASP/ENISA).
- Cloud Computing Security: e.g., how to secure data at rest and protect from honest-but-curious cloud service providers.
- Penetration Testing.
- Cyber forensics: analysis and reporting of computer evidence.

Comparing the results with the second edition (D3.3), the focus shifts from advanced technologies and automation (e.g., *ML with context-awareness* and *DevSecOps*) to foundational cybersecurity topics and best practices such as incident response, data protection, and traditional security controls (e.g., endpoint security, penetration testing). Compared also with the first edition (D3.1), which was used to bootstrap MERIT syllabi, we note how the knowledge blocks tend to narrow (D3.1 listed 39 ones, D3.3 21, and now only 12), with some topics (e.g., Zero Trust) remaining important over time.

Given the many scenarios in which they apply and the potential benefits for their curricula (which would give future MERIT students a leg up), we will also consider the following topics for Step 7 grouping and prioritisation:

- DevSecOps: i.e., integrating security testing at every stage of the software development process.
- Threat modelling: i.e., application and use of well-established frameworks.
- OSINT and Intelligence Analysis: particularly, the basics to become an Intelligence Analyst.
- Security of the software supply chain: e.g., via static and dynamic application security testing in the CI/CD toolchain.
- Security of the AI data pipeline.

The following set provides the **AI** topics, technologies and application areas which are currently leveraged by at least seven organisations participating in AI questionnaires, joined with those indicated by Frost & Sullivan:

- Agentic AI Applications: AI systems that autonomously make decisions, execute tasks, and adapt dynamically. Used in robotics, virtual assistants, and automated research.
- AI Ethics and Governance: Ensures AI development is fair, transparent, and accountable, addressing bias, privacy, and compliance with regulations.



- AI in Smart Manufacturing: Enhances efficiency with predictive maintenance, robotics, quality control, and supply chain optimisation.
- AI in Financial Systems: Improves fraud detection, risk analysis, algorithmic trading, and personalised banking through data-driven models.
- Generative AI Technologies: AI models that create text, images, videos, and code, revolutionising content generation, automation, and scientific applications.
- Skills for AI-Cybersecurity Roles: Requires resilience, adaptability, and expertise in machine learning, cryptography, and network security for AI-driven threat defence.
- AI-Powered Threat Detection: Uses machine learning to analyse behaviour, detect anomalies, and prevent cyber threats in real-time.
- AI-Enhanced Incident Response: Automates threat identification, risk assessment, and mitigation, improving response efficiency.
- AI for Education: Enables personalised learning, automated grading, and AI-driven tutoring systems for improved education outcomes.
- AI in Retail: Optimises customer experience, demand forecasting, inventory management, and cashier-less checkout systems.
- Edge AI for IoT Security: Processes data locally on IoT devices to reduce latency and enhance real-time threat detection.

The following set provides the **IoT** application types currently or planned to be deployed in the regions of organisations participating in Step 5 questionnaires, and those indicated by Frost & Sullivan.

- Agriculture: e.g., animal monitoring and crop management.
- Autonomous Vehicles: e.g., vehicle-to-vehicle communication and remote diagnostics.
- Building Automation: e.g., smart heating and lighting.
- Climate & Sustainability: e.g., emissions monitoring and early warning for natural disaster.
- Energy: e.g., energy saving and smart energy grids.
- Environment & Green Transition: e.g., environmental monitoring and waste management.
- Healthcare: e.g., e-health and fall protection.
- Logistics & Supply Chain: e.g., product tracking and supply chain management.
- Manufacturing: e.g., predictive maintenance.
- Mobility & Transportation: e.g., traffic and parking management.
- Public Safety: e.g., streetlight management, road and infrastructure sensors.
- Robotics, metaverse and mixed reality: e.g., remote surgery and real-time simulations.
- Military: e.g., autonomous reconnaissance and situation awareness.

The following list reports the IoT technologies which are currently used or are going to be used by participants:

- Applied AI.
- Autonomous Systems.
- Cellular IoT (2G/3G/4G/5G).
- Data Ecosystems or Data Spaces.
- Digital Twins.
- Edge Computing.
- Intelligent Sensors.
- IoT-based Analytics.
- IoT Platforms.
- Satellite IoT.
- Wearables.
- Distributed IoT and AI.

Considering the importance of critical infrastructures, we decided to add telecommunications for Step 7 grouping and prioritisation. We also agreed to consider *mixed reality* in addition to the Metaverse.



Compared to the second edition, which includes many "smart" fields (e.g., smart home, smart city and smart industry), the current one covers a wide spectrum of IoT topics and application areas, from well-established ones (e.g., agriculture and healthcare) to newest (IoT in the Metaverse and for military). Compared with the first edition, the current one is more general and less cybersecurity-oriented. The interest in the following technologies persists over time: digital twins, Cellular IoT, IoT for mobility/transportation, Sensors, data management and analytics.

2.7 Step 7 - Merge data analysis and market needs with MERIT universities vision, and prioritise results

Step 7 leverages the set of skills highlighted by consortium Universities (ref. to Step 2), the Scopus database and the expertise of the MERIT consortium members to prioritise the topics, technologies and application areas from Step 6 to update MERIT master programs. In this step, we also verify the coverage of recommended topics and highlight the soft skills that MERIT universities should incentivise. All data is compared with past analyses (D3.3 and D3.1).

Results:

In the **Cybersecurity** domain:

Table 7: Prioritised list of Cybersecurity topics, technologies and application areas for MERIT courses and related activities. "X₁" indicates those in line with Step 2 desiderata, "X₂" those deemed relevant from the Scopus database investigation.

Cybersecurity Topic or Technology to be included in syllabi; Skill or Expertise (in specific application areas) to be developed by students.	To prioritise
Human factors in cybersecurity: e.g., training to protect against social engineering and phishing. (Ref. to query CS-Q1 in the following Scopus database investigation and in Appendix A).	
Zero Trust framework: security measures at the different layers and ways to support them. (Ref. to CS-Q2)	
Practical incident response: e.g., using a well-established Extended Detection and Response (XDR) solution. (Ref. to CS-Q3)	
Data protection and privacy (e.g., pseudonymisation, but also including the privacy- and security-aware use of AI tools). (Ref. to CS-Q4)	X ₂
Cyber Threat Intelligence: particularly, the types of intelligence and how to process and present them. (Ref. to CS-Q5)	
Cyber risk assessment, governance and management tools. (Ref. to CS-Q6)	X ₁ / X ₂
Identity Protection (e.g., multi-factor or risk-based authentication) and Access Management (e.g., managing a privileged access workstation). (Ref. to CS-Q7)	
Endpoint Security Solutions: endpoint detection and response (EDR). (Ref. to CS-Q8)	
Regulatory Compliance (e.g., towards NIS2) and support of well-known best practices (e.g., from OWASP and ENISA). (Ref. to CS-Q9)	X ₁
Cloud Computing Security: e.g., how to secure data at rest and protect from honest-but-curious cloud service providers. (Ref. to CS-Q10)	
Penetration Testing. (Ref. to CS-Q11)	X ₁
Cyber forensics: analysis and reporting of computer evidence. (Ref. to CS-Q12)	
DevSecOps: i.e., the integration of security testing at every stage of the software development process. (Ref. to CS-Q13)	X ₁
Threat modelling: i.e., application and use of well-established frameworks. (Ref. to CS-Q14)	X ₁
OSINT and Intelligence Analysis: particularly, the basics to become an Intelligence Analyst. (Ref. to CS-Q15)	
Security of the software supply chain: e.g., via static and dynamic application security testing in the CI/CD toolchain. (Ref. to CS-Q16)	X ₁
Security of the AI data pipeline. (Ref. to CS-Q17)	

Considering the envisaged set of skills resulting from Step 2, *Regulatory Compliance* more directly aligns with RTU desiderata (considering the legal aspects of system management); *Cyber Risk Assessment, Governance and Management Tools, Penetration Testing* and *Threat Modelling* with UPC one (considering the ability to identify, classify and mitigate security risks, also considering the perspective of an attacker), together with



DevSecOps and *Security of the Software Supply Chain* (considering the development of hardware or software systems with innovative, secure solutions). Those have been indicated with X_1 in the table above.

By investigating the topics, technologies and application areas using the Scopus database (<https://www.elsevier.com/products/scopus>) in the past five years via specific query parameters (ref. to Appendix A), we can observe in Figure 3 a persistent and growing interest in *Cyber Risk Assessment, governance and Management Tools* (Query CS-Q4, 1548 slope⁴ value) and *data protection, pseudonymisation and privacy* (CS-Q6, 1639.7 slope value). Those have been indicated with X_2 .

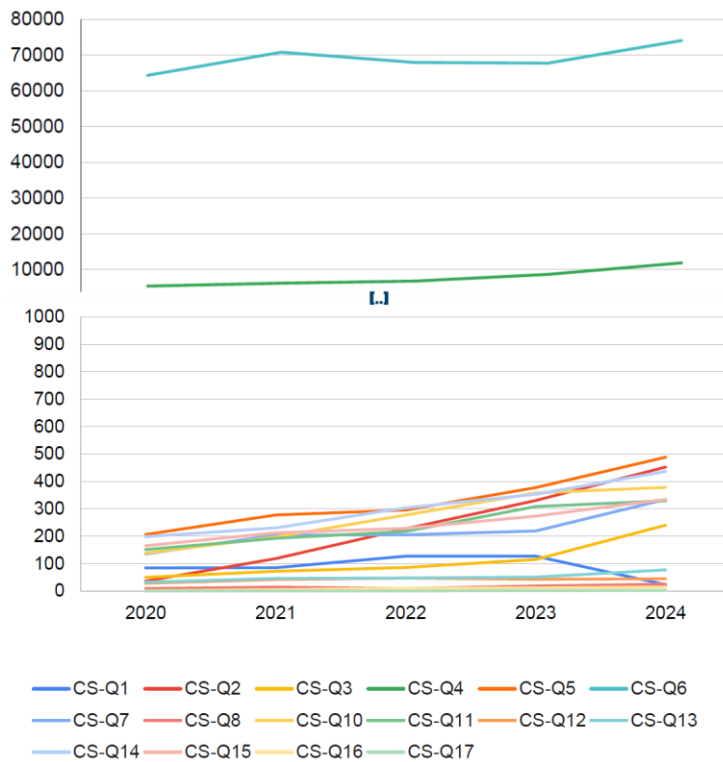


Figure 3: Academic interest in the reported CS topics, technologies and application areas in the past five years using Scopus and specific queries and parameters (ref. to Appendix A).

In the **Artificial Intelligence** domain:

Table 8: Prioritised list of Artificial Intelligence topics, technologies and application areas for MERIT courses and related activities. “ X_1 ” indicates those in line with Step 2 desiderata, “ X_2 ” those deemed relevant from the Scopus database investigation.

Artificial Intelligence Topic or Technology to be included in syllabi; Skill or Expertise (in specific application areas) to be developed by students.	To prioritise
Agentic AI applications: AI systems that autonomously make decisions, execute tasks, and adapt dynamically. Used in robotics, virtual assistants, and automated research. (Ref. to query AI-Q1 in the following Scopus search and in Appendix A).	

⁴ Defined as the vertical distance divided by the horizontal distance between any two points on the line, which is the rate of change along the regression line. Ref. to <https://support.microsoft.com/en-gb/office/slope-function-11fb8f97-3117-4813-98aa-61d7e01276b9>.



AI Ethics and Governance: Ensures AI development is fair, transparent, and accountable, addressing bias, privacy, and compliance with regulations. (Ref. to AI-Q2)	X ₁
AI in Smart Manufacturing: Enhances efficiency with predictive maintenance, robotics, quality control, and supply chain optimisation. (Ref. to AI-Q3)	X ₁
AI in Financial Systems: Improves fraud detection, risk analysis, algorithmic trading, and personalised banking through data-driven models. (Ref. to AI-Q4)	X ₁
Generative AI Technologies: AI models that create text, images, videos, and code, revolutionising content generation, automation, and scientific applications. (Ref. to AI-Q5)	X ₂ .
Skills for AI-Cybersecurity Roles: Requires resilience, adaptability, and expertise in machine learning, cryptography, and network security for AI-driven threat defence. (Ref. to AI-Q6)	X ₁
AI-Powered Threat Detection: Uses machine learning to analyse behaviour, detect anomalies, and prevent cyber threats in real time. (Ref. to AI-Q7)	X ₁
AI-Enhanced Incident Response: Automates threat identification, risk assessment, and mitigation, improving response efficiency. (Ref. to AI-Q8)	X ₁
AI for Education: Enables personalised learning, automated grading, and AI-driven tutoring systems for improved education outcomes. (Ref. to AI-Q9)	X ₂ .
AI in Retail: Optimises customer experience, demand forecasting, inventory management, and cashier-less checkout systems. (Ref. to AI-Q10)	X ₁
Edge AI for IoT Security: Processes data locally on IoT devices to reduce latency and enhance real-time threat detection. (Ref. to AI-Q11)	X ₁

Considering the envisaged set of skills resulting from Step 2, *AI Ethics and Governance* is directly in line with the vision of all MERIT universities (considering “follow ethical standards ..”); *Smart Manufacturing* is aligned with Taltech desiderata (considering the *design and optimisation of integrated manufacturing systems, problem-solving in manufacturing engineering and management, waste reduction, and understanding of production planning and management*). *AI in Financial Systems* (considering “Develop technical systems to solve economic problems [...]”), *Edge AI for IoT Security* (considering “select appropriate tools for IoT projects, evaluate AI, cybersecurity, and IoT solutions [...]”), *AI-Powered Threat Detection* and *AI-Enhanced Incident Response* (considering the development of innovative solutions”), and *Skills for AI-Cybersecurity Roles* follows UPC desiderata; *AI in Retail* follows instead RTU ones (considering – among others – the application of technologies for process efficiency). Those have been indicated with X₁ in the table above.

By investigating the topics, technologies and application areas using the Scopus database, we can observe in Figure 4 a notable interest in *Generative AI* (Query AI-Q5, slope 1543.6) and AI for education (AI-Q9 slope 1962.07) since 2023. Those have been indicated with X₂.

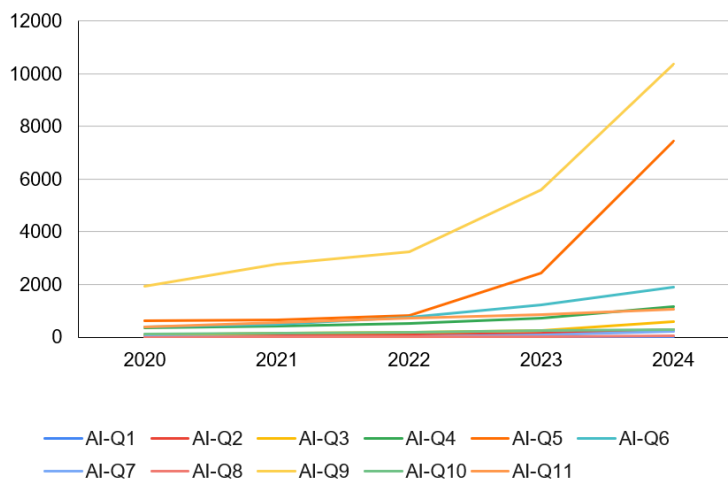


Figure 4: Academic interest in the reported AI topics, technologies and application areas in the past five years using Scopus and specific queries and parameters (ref. to Appendix A).



In the context of **Internet of Things**:

Table 9: Prioritised list of topics, technologies and application areas related to the Internet of Things for MERIT courses and related activities. “X₁” indicates those in line with Step 2 desiderata, “X₂” those deemed relevant from the Scopus database investigation.

Internet of Things Topic or Technology to be included in syllabi; Skill or Expertise (in specific application areas) to be developed by students.	To prioritise
IoT application domains: agriculture, mobility, transportation, building automation, <u>climate, sustainability, energy, environment, green transition, healthcare, logistics, supply chain, manufacturing, telecommunication, public safety, robotics, military, the Metaverse, mixed reality.</u> (Ref. to query IoT-Q1 in the following Scopus search and in Appendix A).	X ₁ / X ₂
IoT security: data management, data ecosystems and data spaces. (Ref. to IoT-Q2)	X ₁ / X ₂
IoT and AI (e.g., autonomous systems). (Ref. to IoT-Q3)	X ₁
Cellular IoT, satellite and wearables. (Ref. to IoT-Q4)	X ₁
IoT at edge: digital twins and edge computing. (Ref. to IoT-Q5)	X ₂
Intelligent sensors and analytics. (Ref. to IoT-Q6)	X ₁
IoT platforms. (Ref. to IoT-Q7)	X ₁

Considering the envisaged set of skills resulting from Step 2, *IoT in manufacturing* and *IoT solutions for logistics and supply chain* are directly related to Taltech and RTU desiderata (considering the *design and optimisation of integrated manufacturing systems*, and the emphasis on *process efficiency and system design in manufacturing engineering and management* – respectively); *IoT for climate and sustainability*, for *environment and green transition* and in the *energy domain* for all MERIT universities in accordance with the objective to allow students to propose sustainable solutions; *IoT and AI (e.g., autonomous systems)* and *Intelligent sensors and analytics* with RTU requirements (considering *AI integration* and *data analytics*); *Cybersecurity and Data Management, IoT platforms, and Cellular IoT, satellite, and wearables* for UPC (with respect to *selecting appropriate tools for IoT* and the focus on *cybersecurity, and studying practical application of IoT solutions*). They have been indicated with X₁ in the table above.

By investigating the topics, technologies and application areas using the Scopus database, we can observe in Figure 5 an increasing interest in IoT at edge (Query IoT-Q5, slope 2938.8) and a fairly stable number of research products in IoT applications (IoT-Q1, slope 1905.1) and IoT security (IoT-Q2, slope 1075.4). Those have been indicated with X₂.

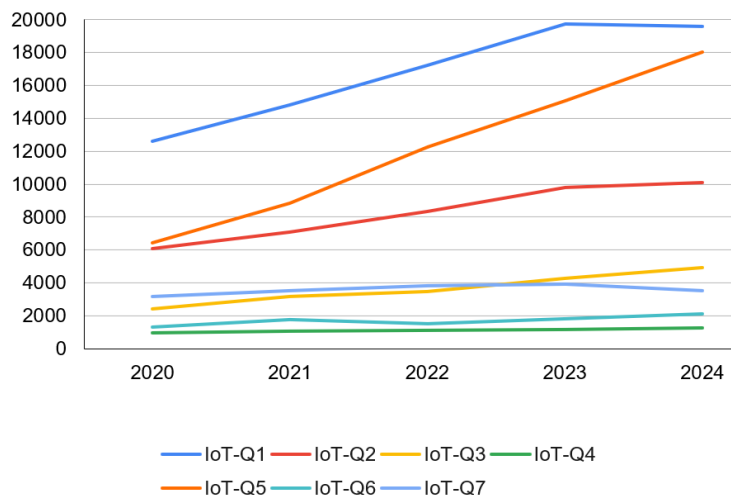


Figure 5: Academic interest in the reported IoT topics, technologies and application areas in the past five years using Scopus and specific queries and parameters (ref. to Appendix A).



Since there are no updates (yet) to the syllabi of the Universities (ref. to Step 2) or recommendations from industry questionnaires, we believe students should be presented with activities supporting the same set of soft skills indicated in the past edition:

Considering the soft skills, MERIT universities should prioritise for the future set of students:

- Leadership: They should be able to lead when necessary.
- Communication: Graduates should be able to communicate effectively in English.
- Understanding Impact: They should understand the impact of proposed solutions.
- Problem-Solving: Problem-solving in manufacturing engineering and management is emphasised.
- Strategy Development: Proficiency in strategy development is expected.
- Teamwork: They should work well in teams.
- Critical Thinking: Graduates are expected to exhibit critical thinking.
- Professional and Ethical Behaviour: Adherence to professional and ethical behaviour principles is expected.
- Understanding Legal and Social Aspects: They should understand the legal and social aspects of system management.
- Continuous Learning: All universities emphasise the importance of continuous learning.
- Ethical Standards: Adherence to ethical standards is expected.

Compared with the past edition, current topics, technologies and areas are more tailored to practical, industry-specific applications, whereas D3.3 recommendations were designed to build a stronger theoretical foundation with extensive technical details, catering to a wider range of career pathways. In detail, the cybersecurity offering now includes the human factor (for instance, how to detect and counter phishing), practical incident response using established XDR solutions, and integrated security measures for AI data pipelines, whereas D3.3 span from secure communication protocols to context-aware machine learning for anomaly detection. In the field of artificial intelligence, the list now includes agentic AI applications, the use of AI in finance, cybersecurity-oriented AI (skills to study and use AI in CS), and edge AI integration. Regarding the Internet of Things, we maintain the same level of knowledge over platforms, services and use cases. This edition confirms the influence of AI in both Cybersecurity and IoT, as highlighted in D3.3. Table 10 list the elements shared (at different levels of coverage) by the current and past Step 7 output:

Table 10: Step 7 results shared between D3.4 and D3.3.

Cybersecurity	Artificial Intelligence	Internet of things
<ul style="list-style-type: none"> ○ Zero Trust (framework/principles). ○ Threat Modelling. ○ DevSecOps (integration of security in development). ○ Penetration Testing. ○ Incident Response/Management. ○ Risk Management and Governance. ○ Cloud Computing Security. ○ Identity Protection/Advanced Authentication Procedures. 	<ul style="list-style-type: none"> • Generative AI (technologies/tools). • AI Ethics and Governance (ethical issues). • AI Applications in Education (e.g., personalised or higher education approaches). • AI Applications in Manufacturing (smart manufacturing practices). 	<ul style="list-style-type: none"> • IoT Platforms and Services. • Data Ecosystems and Data Spaces. • Edge Computing (including digital twins). • Intelligent Sensors and Analytics. • Cellular IoT. • Applications in Smart Transportation and Healthcare.



To verify the current integration of Table 7 (for CS), Table 8 (AI) and Table 9 (IoT) topics, technologies, and applications areas in the MERIT master programs, we adopted as in D3.1/D3.3 the strategy described in the MERIT Milestone MS6.

Upon 35 entries (corresponding to Table 4, Table 5 and Table 6 rows), 22 were covered by at least one of the courses from MERIT universities (two by all universities, AI-Q1 and AI-Q2). This highlights the need for MERIT universities to intervene in updating course contents and share available resources to reflect the new requirements. In contrast to this edition, in the previous one we found a more widespread coverage of topics, technologies and application areas.

To understand how the results of the third edition of the methodology align with the European skills and labour market, we assessed as in D3.1/D3.3 their adherence to the European Skills, Competences, Qualifications and Occupations (**ESCO**) [26] classification, and to the European e-Competence Framework (e-CF) [27].

To identify which ESCO Skills, Knowledge, and Occupations our results relate to, we queried (as in D3.1) the ESCO database via the local API using the 35 keywords from Step 7 and the *Full Text Search* API. In this edition, we obtained 7730 results (4057 unique), which could be a *Concept*, *Skill*, or *Knowledge* item in the ESCO classification and may be associated with zero or more occupations. We carefully reviewed them to exclude those out of context and obtained a list of 590 results (26 related to the AI domain, 202 and 362 to CS and IoT ones, respectively). Using the script⁵ developed for the first application of the methodology we obtained 587 low-level items:

- 330 unique skills: 129 associated with the CS domain, 15 with AI, and 215 with IoT.
- 202 unique knowledge items: 72 in the CS domain, 11 in AI, and 145 in IoT.

Considering the parent items:

- 97 unique skills: 53 in the CS domain, 59 in AI, and 44 in IoT.
- 43 unique knowledge items: 19 in the CS domain, 4 in AI and 37 in IoT.

According to the ESCO classification, the knowledge of topics, technologies, and skills identified in Step 7 would enable MERIT students to access 1602 possible occupations (945 related to CS, 65 to AI, and 1009 to IoT).

Comparing those results with the second application of the methodology, we have approximately the same number of unique knowledge and skills items (569 in the second edition, 532 now – 392 in D3.1).

Regarding the **e-CF framework**, we mapped which of its roles could be associated with Step 7 results and at which skill level (among the defined skill groups).

- Human factors in cybersecurity – D.3 (L2, L3), D.9 (L2).
- Zero Trust framework – D.1 (L4, L5), E.8 (L4).
- Practical incident response – C.4 (L2, L3), E.8 (L3).
- Data protection and privacy – D.1 (L4, L5), E.8 (L4).
- Cyber Threat Intelligence – D.7 (L3, L4), D.10 (L3).
- Cyber risk assessment, governance and management tools – A.1 (L4, L5), D.1 (L4, L5), E.3 (L3), E.9 (L4).
- Identity Protection and Access Management – D.1 (L4, L5), E.8 (L4).
- Endpoint Security Solutions (EDR) – D.1 (L4, L5), E.8 (L3).
- Regulatory Compliance (e.g., NIS2, OWASP/ENISA) – D.1 (L4, L5), E.9 (L4).
- Cloud Computing Security – D.1 (L4, L5), A.5 (L3, L4), E.8 (L4).
- Penetration Testing – B.3 (L3), E.8 (L3).
- Cyber forensics – C.4 (L3, L4), E.8 (L3).

⁵ Available at https://digitalmerit.eu/wp-content/uploads/2024/07/MERIT_ESCO_code.zip.



- DevSecOps – B.1 (L3), B.3 (L2, L3), E.5 (L3).
- Threat modelling – D.1 (L4, L5), A.5 (L3, L4), E.3 (L3).
- OSINT and Intelligence Analysis – D.7 (L2, L3), D.10 (L3).
- Security of the software supply chain – B.3 (L3), E.3 (L3).
- Security of the AI data pipeline – D.1 (L4, L5), A.5 (L3, L4), E.8 (L4).
- Agentic AI applications – A.9 (L4, L5), A.7 (L3, L4), E.7 (L3).
- AI Ethics and Governance – D.1 (L4, L5), E.9 (L4).
- AI in Smart Manufacturing – A.9 (L4, L5), D.7 (L3, L4), E.1 (L3), E.5 (L3).
- AI in Financial Systems – D.7 (L4, L5), E.3 (L4).
- Generative AI Technologies – A.9 (L4, L5), D.7 (L3, L4), E.1 (L3).
- Skills for AI-Cybersecurity Roles – D.3 (L2, L3), D.9 (L3).
- AI-Powered Threat Detection – D.7 (L4, L5), D.1 (L4, L5), E.8 (L4).
- AI-Enhanced Incident Response – D.1 (L4, L5), D.7 (L3, L4), E.8 (L4).
- AI for Education – A.10 (L2, L3), D.11 (L3).
- AI in Retail – A.9 (L4, L5), D.7 (L3, L4), A.10 (L2, L3), E.1 (L3), D.11 (L3).
- Edge AI for IoT Security – D.1 (L4, L5), D.7 (L3, L4), A.5 (L3, L4), E.8 (L4).
- IoT application domains – A.7 (L3, L4), A.9 (L4, L5), E.1 (L3).
- IoT security – D.1 (L4, L5), A.5 (L3, L4), E.8 (L4).
- IoT and AI (e.g., autonomous systems) – A.7 (L3, L4), A.9 (L4, L5), E.7 (L3).
- Cellular IoT, satellite and wearables – A.7 (L3, L4), E.1 (L3).
- IoT at the edge: digital twins and edge computing – A.5 (L3, L4), A.7 (L3, L4), E.5 (L3).
- Intelligent sensors and analytics – D.7 (L3, L4), A.5 (L3, L4), D.10 (L3).
- IoT platforms – B.6 (L3, L4), A.5 (L3, L4), E.9 (L4).

Those allow the partial/complete coverage of the following e-CF roles:

- Account Manager* (missing e-Competences D5, D6, E4).
- Business Analyst* (missing A3).
- Business Information Manager* (missing A3, E4).
- Chief Information Officer* (missing A3, E2, E4).
- Database Administrator* (missing B2, C2).
- **Data science.**
- Data specialist* (missing A6, E6).
- Developer* (missing B2, B5).
- Devops expert* (missing B2, B4, C2).
- Digital Media Specialist* (missing A6, B4, D6).
- Digital Transformation Leader* (missing A3).
- Enterprise Architect* (missing A3).
- ICT Operations Manager* (missing E2, E6).
- **ICT Security Manager.**
- **ICT Security Specialist.**
- Network Specialist* (missing A6, B2, B4).
- Product Owner* (missing A4, E4).
- Project Manager* (missing A4, E2, E4).
- Quality Assurance Manager* (missing D2, E6).
- Scrum Master* (missing E4).
- Service Manager* (missing A2, C3, D8).
- Service Support* (missing C1, C2, C3).
- Solution Designer* (missing A6).
- Systems Administrator* (missing B2, C2).
- Systems Analyst* (missing B5, E6).
- Systems Architect* (missing B2).
- Technical Specialist* (missing C2, C3, E6).
- Test Specialist* (missing B2, B5).



Compared with past editions, the list does not cover B4, C2, C3, C5, and E2 (with respect to D3.3) and B2, C4, and D6 (with respect to D3.1).

3 Roles of AI-CS and AI-IoT

Artificial Intelligence (AI) is transforming multiple domains, offering both opportunities and challenges. In higher education, AI enhances personalised learning and administrative efficiency while raising concerns about ethical adoption, addressed through the CRAFT framework. In cybersecurity, AI serves as both a tool for defence and a weapon for cybercriminals, necessitating stronger security measures. In this section, we highlight the latest roles, skills, and technologies that are essential for staying competitive in the evolving AI landscape.

Artificial Intelligence (AI) in Cybersecurity:

- **AI-Powered Threat Detection:** predictive analytics, anomaly detection, malware recognition, and real-time intrusion prevention.
- **Generative AI:** used in phishing simulation, automated security audits, and adversarial attack generation.
- **AI for Incident Response:** tools for automating remediation and mitigating risks after breaches.
- **Adversarial AI:** securing AI systems from evasion attacks, data poisoning, and model exploitation.
- **AI-driven SOC (Security Operations Center):** enhancing log analysis, risk assessment, and alert prioritisation.
- **Explainable AI (XAI):** for transparency in automated decisions affecting cybersecurity measures.
- **AI-enhanced Vulnerability Scanning:** automated scanning, prioritising threats, and patching weak points.
- **Quantum AI:** threat to current encryption methods; future cryptography research.
- **Large Language Models (LLMs):** fraud and social engineering defence, especially in text-based attacks.

Artificial Intelligence Roles in Cyber Security:

- **AI Cybersecurity Specialist:**
 - Develop AI models for threat detection.
 - Automate incident responses using AI-driven tools.
 - Secure AI systems from adversarial attacks.
 - Conduct ethical hacking and penetration testing with AI.
- **IoT Security Analyst:**
 - Implement AI-driven security frameworks for IoT networks.
 - Monitor device behaviour and detect anomalies using AI.
 - Design encryption and access management protocols powered by AI.
 - Maintain the integrity of IoT device communications.
- **AI Engineer for IoT Systems:**
 - Build Edge AI models for IoT applications.
 - Optimise IoT systems for predictive maintenance using AI analytics.
 - Develop and test AI-based digital twin simulations.
- **AI Risk and Compliance Officer:**
 - Ensure AI models in cybersecurity adhere to ethical guidelines.
 - Design governance frameworks for AI applications in IoT and cybersecurity.
 - Mitigate risks associated with AI technologies.



AI in IoT (Internet of Things):

- **Edge AI:** on-device AI for real-time data processing in IoT devices, reducing latency and improving decision-making.
- **IoT Security Frameworks:** AI-based anomaly detection in interconnected devices.
- **Digital Twins:** AI-powered virtual replicas of IoT systems for system behaviour predictions and simulations.
- **IoT Analytics:** AI-driven insights for predictive maintenance and performance optimisation.
- **AI-enhanced IoT Encryption:** dynamic encryption for securing IoT data and communication channels.

Skills Needed for AI in Cybersecurity and IoT:

- **Technical Skills:**
 - Machine Learning (ML) and Deep Learning (DL) frameworks (e.g., TensorFlow, PyTorch).
 - Knowledge of cybersecurity concepts like SOC operations, zero trust, and penetration testing.
 - Understanding of adversarial machine learning techniques.
 - Proficiency in programming languages (e.g., Python, R) for AI and cybersecurity tool development.
 - Knowledge of IoT protocols (e.g., MQTT, CoAP) and embedded systems.
- **Analytical Skills:**
 - Data analysis for threat detection and performance optimisation.
 - Predictive analytics and risk assessment.
 - Vulnerability management and prioritisation.
- **Soft Skills:**
 - Ethical decision-making for AI use.
 - Communication of complex AI findings to non-technical stakeholders.
 - Collaboration in cross-functional teams for cybersecurity incident response and IoT deployment.

In Figure 6, we provide the reference framework to help identify key roles, essential technologies, and critical skills required for AI implementation across various industries. It outlines the foundational components enabling AI, the diverse applications of AI, and the specific expertise needed for different roles in the AI ecosystem.

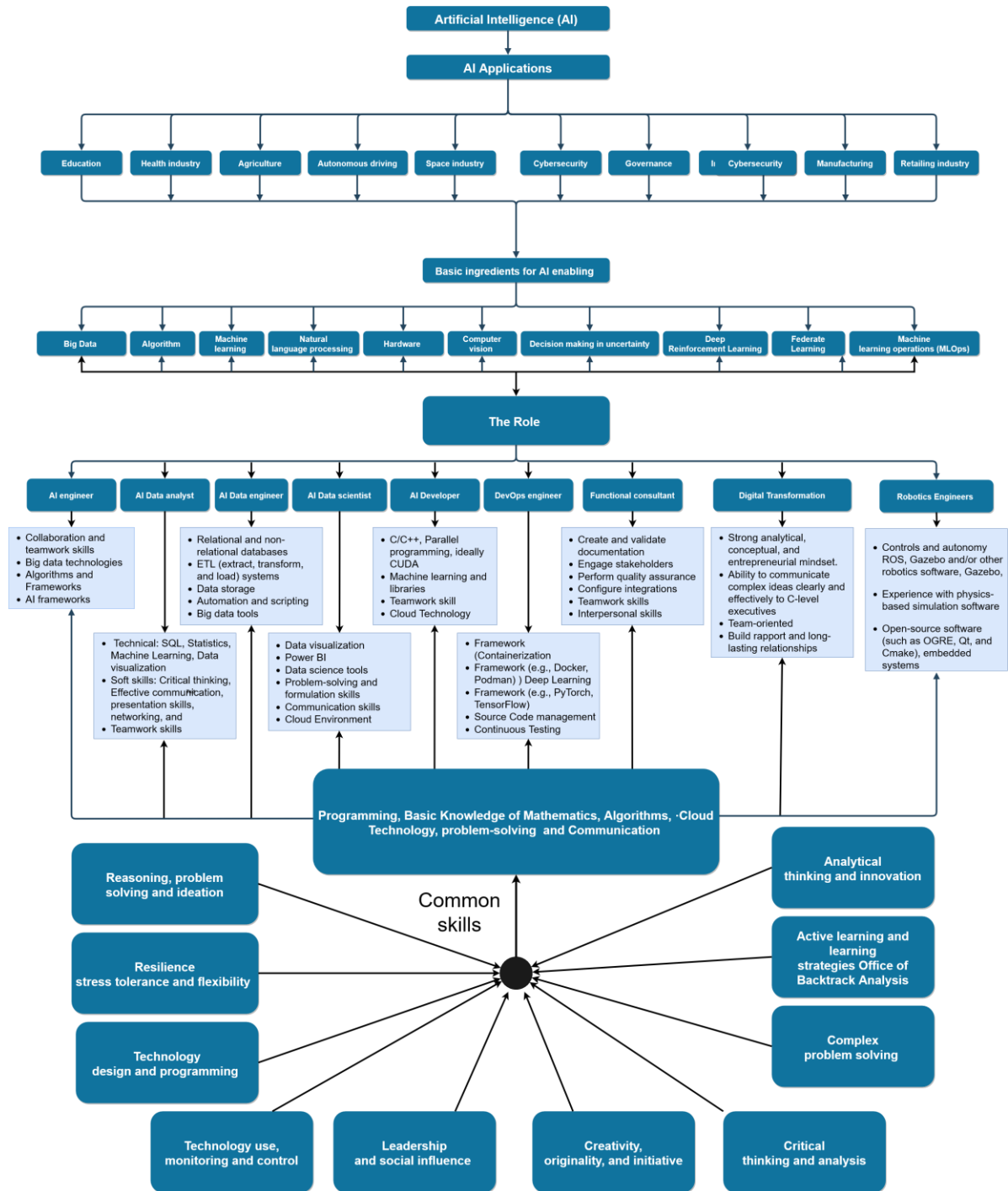


Figure 6: Framework for AI roles, common skills, and specific skills in age of industrial data space.



4 Conclusion

This third iteration of the methodology reinforces the interdisciplinary approach of MERIT master programs, facilitating expertise exchange across AI, CS, and IoT. It also highlights the gap between research and industry in adopting advanced technologies, emphasising the need to expand survey samples. Standardised frameworks, such as ENISA's European Cybersecurity Skills Framework (ECSF) [28], are crucial in defining professional roles and addressing skill gaps. To bridge these gaps, this document provides a structured framework for identifying and prioritising key topics and competencies in the AI, Cybersecurity, and IoT domains, ensuring that MERIT master programs remain aligned with industry demands and technological advancements. The methodology leverages MERIT partners' expertise in research, teaching, laboratory hosting, and prototyping, combining an analysis of current and emerging trends with insights from the industry. This approach produces six concrete results, offering practical guidance for universities in curriculum development, SMEs in workforce upskilling, and research centres in identifying new research areas:

1. The current MERIT partners' areas of expertise, that allowed focusing their effort on identifying the current and forecasted topics, technologies and application areas in the three domains, and can also be used when preparing and updating the material for the master programme (MERIT WP5), and for both the educators upskilling and their mobility between Universities (WP6).
2. A new carefully crafted set of data sources for the AI, CS and IoT domains, created considering only those providing recent and relevant products. The list includes academic portals, and local and globally distributed entities.
3. A set of 71 topics, technologies and scenarios identified from research, statistics, reports and forecasts that are crucial to updating the MERIT master programs (and related activities) to train the next generation of experts in the fields of AI, CS, and IoT and their interplays.
4. A set of 46 topics, technologies and application areas adopted currently or up to the next two years by 35 SMEs inquired via questionnaires in MERIT partners' regions, highlighting the current industry needs. Those are essential to make the study programs operational.
5. A carefully defined mapping of topics, technologies and application areas with the industry needs to highlight those with interest from both industry and academia: 19 possible CS, 20, AI and 16 IoT topics, technologies and 30 application areas.
6. A prioritised list of 30 topics and technologies, and 6 application areas that can be used update the MERIT study program and related activities.
 - a. Evaluating the list in the context of the ESCO [26] framework, we found that the acquisition of these knowledge, technologies and skills is linked with 330 unique skills and 202 knowledge items, spans multiple application areas (from finance to healthcare) and provides access to 1602 job positions.
 - b. Considering the e-CF framework, we mapped Step 7 results to 20 e-CF competences and leveraging competences to 28 e-CF roles.



References

- [1] D. Zowghi and C. Coulin, "Requirements Elicitation: A Survey of Techniques, Approaches, and Tools," in *Engineering and Managing Software Requirements*, 2005.
- [2] McKinsey Digital, "Technology Trends Outlook 2024," 2024.
- [3] S. Morgan, *Cybercrime To Cost The World \$9.5 trillion USD annually in 2024*, 2023.
- [4] CLUSIT, "Rapporto 2024 sulla sicurezza ICT in Italia," 2024.
- [5] Microsoft, "Microsoft Digital Defense Report 2024," 2024.
- [6] A. Folorunso, T. Adewumi, A. Adewa, R. Okonkwo and T. N. Olawumi, "http://dx.doi.org/10.30574/gjeta.2024.21.1.0193," 2024.
- [7] J. Greis and M. Sorel, "The cybersecurity provider's next opportunity: Making AI safer," 2024. [Online]. Available: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer>.
- [8] Gartner, "Top 9 Trends in Cybersecurity for 2024," 2024. [Online]. Available: <https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends>.
- [9] IBM, "Cost of a Data Breach Report 2024," 2024.
- [10] A. Folorunso, T. O. Adewumi, A. Adewa, R. Okonkwo and T. N. Olawumi, "Impact of AI on cybersecurity and security compliance," 2024.
- [11] MCKinsley, "The cybersecurity provider's next opportunity: Making AI safer," 2024.
- [12] World Economic Forum and Accenture, "Global Cybersecurity Outlook 2025," 2025.
- [13] ENISA, "ENISA Threat Landscape 2024," 2024.
- [14] FORBES, "Cybersecurity Trends And Priorities To Watch For 2025," 2024.
- [15] SPLUNK, "CISO REPORT 2025".
- [16] MCKinsley, "MCKinsley Technology Trends Outlook 2024," 2024. [Online]. Available: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech>.
- [17] The EU REWIRE Project, "Job Analyzer," 2025. [Online]. Available: <https://cyberability-platform.informacni-bezpecnost.cz/job-ads-analyzer>.
- [18] The European Commission, "Europe's Internet of Things Policy," 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy>.
- [19] SPD Technology, "AI and IoT: A New Era of Technological Integration," 2024. [Online]. Available: <https://spd.tech/artificial-intelligence/ai-and-iot-a-new-era-of-technological-integration/>.
- [20] IoT Analytics, "IoT 2024 in review: The 10 most relevant IoT developments of the year," 2024. [Online]. Available: <https://iot-analytics.com/iot-2024-review/>.
- [21] IoT Analytics, "State of IoT Spring 2024: 10 emerging IoT trends driving market growth," 2024. [Online]. Available: <https://iot-analytics.com/state-of-iot-10-emerging-iot-trends-driving-market-growth/>.



- [22] E. Fazeldehkordi and G. Tor-Morten , “A Survey of Security Architectures for Edge Computing-Based IoT,” 2022.
- [23] Frost & Sullivan, “Growth Opportunities in the Global Security Awareness Training Industry,” 2022.
- [24] Global Information & Communications Technologies Research Team at Frost & Sullivan, “Insights for CISOs— Preparing for the Dual Nature of Generative AI: Threats and Advantages of GenAI are Changing the Threat Landscap,” 2023.
- [25] Frost & Sullivan's Global 360° Research Team, “Macroeconomic Transformations and the Future of Economy, Business, and Society: Labor Market Shifts, Geopolitical Fragmentation, and Supply Chain Reorientation Will Reshape the Global Economic Landscape,” 2024.
- [26] The European Commission, “European Skills, Competences, Qualifications and Occupations (ESCO),” [Online]. Available: <https://esco.ec.europa.eu/en>.
- [27] European Committee for Standardization (CEN), “European e-Competence Framework (e-CF),” [Online]. Available: <https://ecfexplorer.itprofessionalism.org/>.
- [28] ENISA, “European Cybersecurity Skills Framework (ECSF) - User Manual,” 2022.



Appendix A

The following lists provide the queries for the investigation via Scopus of the topics, technologies or application areas provided in the Step 7 of the methodology and leverages the quotes for exact match and the AND/OR logical operators.

Cybersecurity domain:

- 1 ("cybersecurity" OR "cyber security") AND "Human factor"
- 2 "Zero Trust"
- 3 ("cybersecurity" OR "cyber security") AND "incident response"
- 4 "data protection" OR "data privacy"
- 5 "Threat Intelligence"
- 6 "risk assessment" OR "risk governance" OR "risk management"
- 7 "Identity Protection" OR "Access Management"
- 8 "Endpoint Security"
- 9 ("cybersecurity" OR "cyber security") AND "regulation" AND "compliance"
- 10 ("cybersecurity" OR "cyber security") AND "cloud computing"
- 11 "Penetration Testing"
- 12 "Cyber forensics"
- 13 "DevSecOps"
- 14 "Threat modelling"
- 15 "OSINT" OR "Intelligence Analysis"
- 16 ("cybersecurity" OR "cyber security") AND "software supply chain"
- 17 ("cybersecurity" OR "cyber security") AND "artificial intelligence" AND "data pipeline"

Artificial intelligence domain:

- 1 "artificial intelligence" AND "agentic"
- 2 "artificial intelligence" AND "ethics" AND "governance"
- 3 "artificial intelligence" AND "smart manufacturing"
- 4 "artificial intelligence" AND ("financial systems" OR "finance")
- 5 "artificial intelligence" AND "generative"
- 6 "artificial intelligence" AND ("cyber security" OR "cybersecurity")
- 7 "artificial intelligence" AND "threat detection"
- 8 "artificial intelligence" AND "incident response"
- 9 "artificial intelligence" AND "education"
- 10 "artificial intelligence" AND "retail"
- 11 "artificial intelligence" AND "edge computing"

Internet of things domain:

- 1 "internet of things" AND (agriculture OR "mobility" OR "transportation" OR "building automation" OR "climate" OR "sustainability" OR "energy" OR "environment" OR "green transition" OR "healthcare" OR "logistics" OR "supply chain" OR "manufacturing" OR "public safety" OR "robotics" OR "military" OR "metaverse" OR "mixed reality")
- 2 "internet of things" AND ("security" OR "data management" OR "data ecosystems" OR "data spaces")
- 3 "internet of things" AND ("artificial intelligence" OR "autonomous systems")
- 4 "internet of things" AND ("cellular" OR "satellite" OR "wearables")
- 5 "digital twins" OR "edge computing"
- 6 "intelligent sensors" OR ("internet of things" AND "analytics")
- 7 "internet of things" AND "platforms"



Appendix B

The following is an abstract representation of the script created to query the ESCO database via the local API.

1. Define a function to read keywords from a file.
2. Define a function to determine the concept type based on the concept string.
3. Define a function to get the KLST (Knowledge, Skills, and Tasks) for a given keyword and group:
 - i. Send a request to a local server with the keyword.
 - ii. Parse the response and extract the results.
 - iii. For each result, check if it matches the keyword.
 - iv. If it does, add any associated occupations to a global list.
 - v. Determine the type and parent of the keyword based on the result data.
 - vi. Return a list containing the group, keyword, type, parent title, and parent code.
4. Initialize a dictionary to store occupations for different groups.
5. Get a list of all text files in the current directory.
6. For each file, read the keywords, get the KLST for each keyword, and write the results to a CSV file.
7. For each group in the occupations dictionary, write the occupations to a separate CSV file.