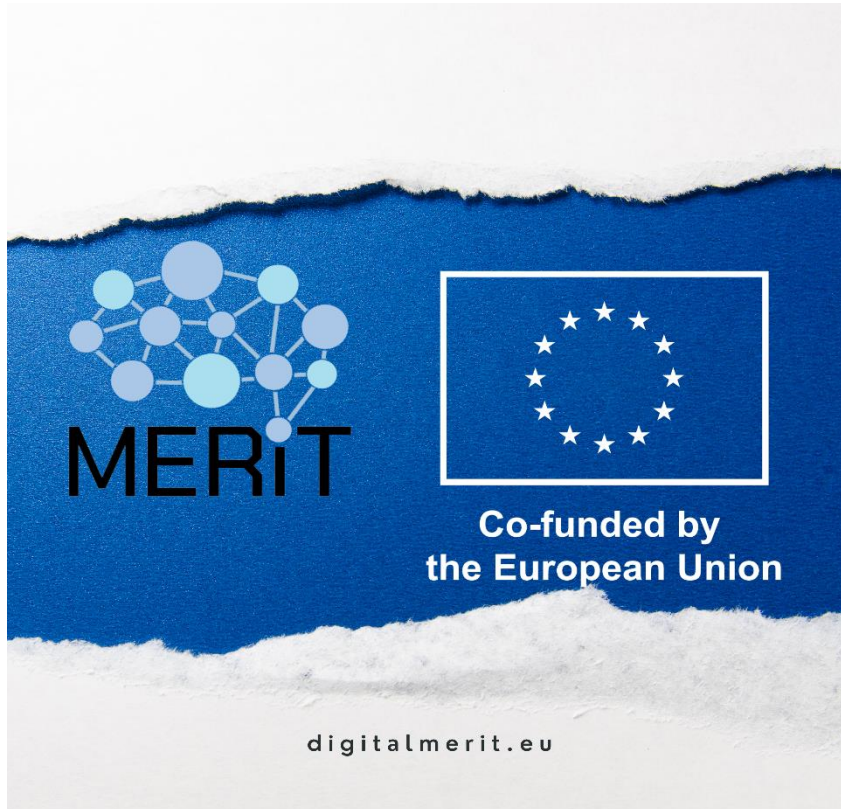




MERIT Deliverable



**Co-funded by
the European Union**



D.3.3 - Annual market and state of the art analysis in the context of IoT, AI and Cybersecurity: Second year.

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

Project Start Date: October 1st, 2022

Duration: 48 months

Call: DIGITAL-2021-SKILLS-01

Date of delivery: 31/03/2024

Topic: DIGITAL-2021-SKILLS-01-SPECIALISED

Dissemination Level: Public



Grant Agreement Number:	101083531
Project Title:	Master of Science in Smart, Secure, Interconnected Systems
Project Acronym:	MERIT
Document Number:	D3.3
Document Title:	Annual market and state of the art analysis in the context of IoT, AI and Cybersecurity: First year
Version:	2.0
Delivery Date:	16/07/2024
Lead Beneficiary:	FBK
Editor(s):	Umberto Morelli (FBK)
Authors:	Umberto Morelli, Imran Muhammad, Federico Lenzi, Diego Sona
Reviewers:	Larisa Survilo (RTU), Agris Nikitenko (RTU), Edgaras (SSMTP), Kristo Karjust (TalTech), Egidijus Pilypas (Exacaster), PMB (Sara Hortal - UPC , Simona Ramanauskaitė – VilniusTech).
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), Diego Sona (FBK)	19.03.2023
0.2	Content review	Larisa Survilo (RTU), Agris Nikitenko (RTU)	20.03.2023
0.3	Content review	Kristo Karjust (TalTech)	24.03.2024
0.4	Content review	Egidijus Pilypas (Exacaster)	25.03.2024
0.5	Content review	PMB (Sara Hortal - UPC, Simona Ramanauskaitė – VilniusTech)	26.03.2024
1.0	Final version	Integration of reviewers and PMB suggestions.	27.03.2024
2.0	Mapping of the results to the ESCO and e-CF frameworks: update of the <i>Executive Summary</i> (pg. 6), <i>Methodology</i> (Step 7, pg. 34-36), <i>Conclusions</i> (pg. 41) and addition of <i>Appendix B</i> (pg. 47)	Umberto Morelli, Muhammad Imran (FBK)	16.07.2024



Table of Contents

LIST OF FIGURES	5
LIST OF TABLES.....	5
EXECUTIVE SUMMARY	6
1 INTRODUCTION	7
2 METHODOLOGY	8
3 ROLES OF AI-CS AND AI-IOT	37
4 CONCLUSIONS	41
REFERENCES	43
APPENDIX A.....	46
APPENDIX B.....	47



List of Figures

Figure 1: Methodology to investigate current state-of-the-art and forecasted topics, skills and technologies from both research and industry perspectives; and including Universities' needs.	8
Figure 2: Word cloud generated from MERIT HEIs 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).	31
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).	32
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).	33
Figure 6: Framework for AI roles, common skills, and specific skills in age of industrial data space.	40

List of Tables

Table 1: MERIT Partners' areas of expertise.	9
Table 2: List of data sources, their field and scope.	11
Table 3: Prioritised list of Cybersecurity topics, technologies and application areas for MERIT courses and activities.	29
Table 4: Prioritised list of Artificial Intelligence topics, technologies and application areas for MERIT courses and activities.	31
Table 5: Prioritised list of Internet of Things topics, technologies and application areas for MERIT courses and activities.	32



Executive Summary

This document presents the Deliverable 3.3 (D3.3) of the MERIT Work Package 3 (WP3): the second-year analysis of market needs, state-of-the-art and innovative approaches, and technologies in Artificial Intelligence (AI), Cybersecurity (CS) and Internet of Things (IoT) domains. It follows the methodology defined with Deliverable 3.1 (D3.1 - the first-year analysis) to validate D3.1 results and identify new topics, trends and technologies to support MERIT activities.

The results of the second application of the methodology are the following:

1. The new, updated areas of expertise of MERIT consortium;
2. The updated envisaged set of skills for students enrolled in MERIT partner's HEIs, created from their master programmes syllabi;
3. The updated data sources and keywords identified by the MERIT consortium to investigate current and forecasted topics and skills in AI, CS and IoT;
4. A new set of topics and skills 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;
5. A set of technologies derived from three questionnaires (AI, CS, and IoT) administered to organisations in MERIT partners regions to investigate regional needs - a key enabler to make the skills of the study program operational;
6. A carefully defined mapping from topics to technologies that facilitates the exploitation of the skills developed during the study program;
7. A prioritized list of topics, skills and technologies that can be used to update and complement MERIT courses contents and related activities. As with D3.1, the list is mapped to the skills, knowledge and occupations associated with the EU ESCO and e-CF frameworks to highlight its applicability and potential in the European context.

The goals of the document are: (I) guide the upgrade of the MERIT master programmes to support current and future industry needs with graduates highly specialized in the most relevant AI, CS and IoT topics; (II) impact the society in line with the activities of the MERIT communication and dissemination strategy, involve regional SMEs in the process to help filling potential regional skill gaps and future dissemination events; (III) increase the expertise of consortium members from both the research and industry perspectives.

The first edition of D3.1 was published in Month 6 (M6) and updated now (M18) and yearly (M30 and M42) to reflect the evolving requirement landscape of the market and research dimensions.

The application of the strategy provides input to the design and upgrade of the study programs contents (associated with WP5 and WP6) and related communication and dissemination activities (associated with WP2).



1 Introduction

WP3 aims to provide the MERIT long-term strategy and identify the most relevant topics for the master programme and related activities, such as hackathons or public outreach events. It operates at three levels:

- Design of the master programme (in the first edition) - feeding the identified topics, skills and technologies to WP4 (tasks in this working package have ended) for their teaching/support by tailoring the master programme's structure.
- Development of the programme material - understanding the expertise in the consortium to later distribute responsibilities over the preparation of courses and activities about identified topics, skills and technologies (WP5).
- Administration of the programme - with the possible upskilling of educators or SME employees on identified topics, skills and technologies (WP6).

In addition, WP3 coordinates with WP2 to advance digital skills among its identified target groups, with specific actions to communicate and disseminate the current and future most relevant topics, skills and technologies.

The following specific objectives have been defined for this WP:

- Increase the reputation of consortium universities as leaders in Artificial Intelligence (AI), Cybersecurity (CS) and Internet of Things (IoT) areas, thus becoming a close-by expert to the society and industry of digital competencies.
- Update the teaching staff skills through knowledge and synergy received from the collaboration of different stakeholders.
- Stimulate the growth of advanced digital skills in Europe by attracting additional target groups to choose AI, IoT and Cybersecurity master studies or individual courses to broaden and deepen the set of required skills to tame the challenges and complexity of current and next generation systems.

To fulfil these objectives, D3.3 applies the methodology developed for the first-year analysis (in D3.1) to identify the most relevant topics, skills, and technologies in the context of AI, CS and IoT, from both market and research perspectives; and to obtain a new prioritised list of topics to update the MERIT master programs and related activities. Results are compared at each step with the first-year analysis.

Organisation of the document

The document is organised as follows. Section 2 presents the seven-steps methodology to identify the skills and topics, and its second application (comparing the results with those from the first-year edition). Section 3 provides the updated set of skills requested by the specialised job positions leveraging both 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.

2 Methodology

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

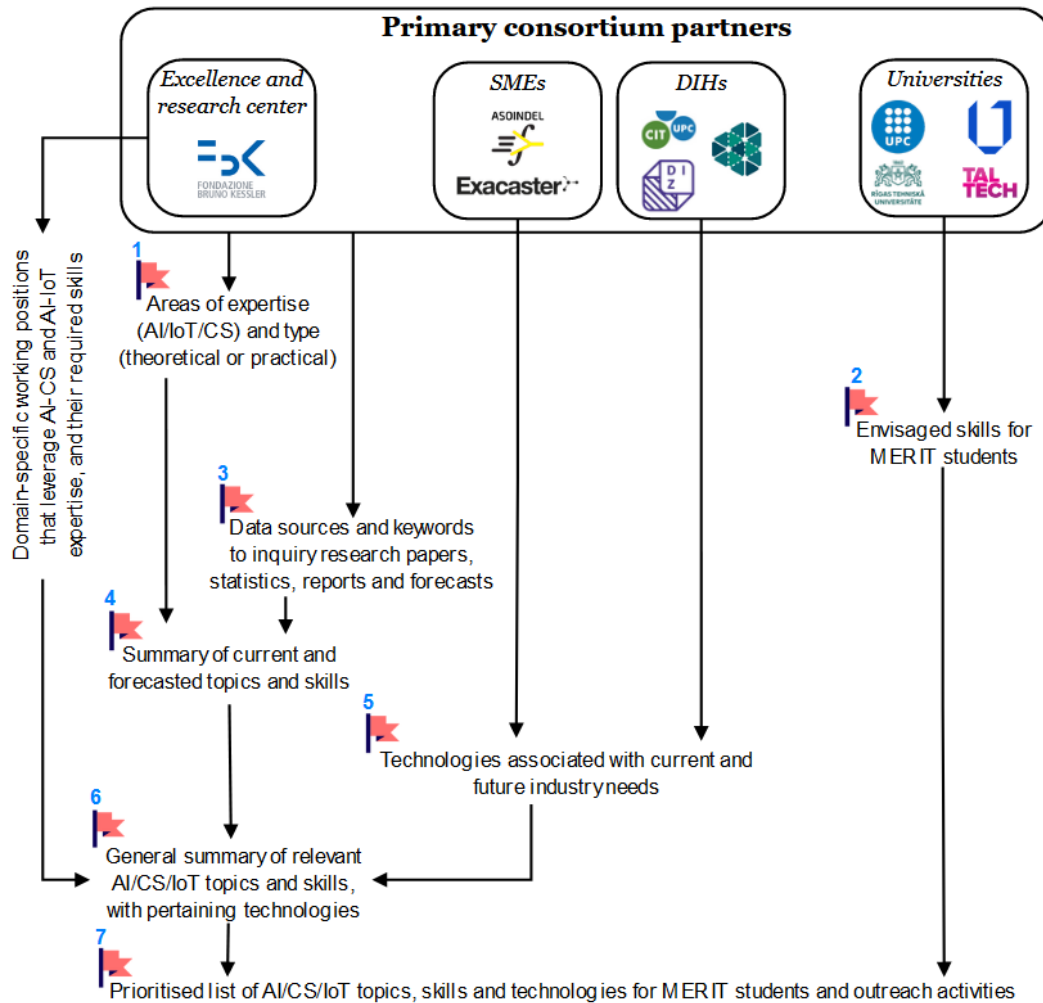


Figure 1: Methodology to investigate current state-of-the-art and forecasted topics, skills and technologies from both research and industry perspectives; and including Universities' needs.

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; 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 to the state-of-the-art analysis in literature, SMEs and DIHs to inquiry industrial needs); and considers the specific Universities' needs to prioritise identified topics and skills.



Approach

To understand the relevant set of topics, skills and technologies for MERIT students (and a broader audience in accordance with future MERIT outreach and upskilling activities) the consortium followed the methodology developed in deliverable D3.1 (which was inspired by the requirement elicitation process reported in [1]). We provide in the following the seven steps and their new results, comparing them with the first-year edition.

Step 1) Request each MERIT partner their **area of expertise** to focus contributions to the state-of-the-art investigation. The goal was to create three groups 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/skills. We underline in the table the newly available expertise from the first-year edition and cross those not available anymore; “*” indicates they will soon be available.

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	<u>R</u> , <u>T</u> , P, <u>L</u> *	<u>R</u> , <u>T</u> , <u>P</u> *, <u>L</u>	R, T, P, L
Vilnius tech	R, T, <u>P</u>	R, T, L	R, T, L
RTU	R, T, P, L	<u>R</u> , <u>T</u> , <u>L</u>	R, T, P, L
TalTech	R, T, <u>P</u>	R, T	R, T, P, L
Exacaster	R, P		
Asoindel	R, <u>P</u>		<u>R</u> , T, P, L
DIZNE	R, T , P	<u>R</u> , T , P	<u>R</u> , T , P
SSMTP	T	T, L	
CIT-UPC	R	<u>R</u>	R

Comparing the table with the first application of the methodology, the MERIT consortium increased their skills in the three domains (8 new expertise).

Step 2) Request each University the set of **mandatory skills** they want their students to develop, to guide the investigation and later prioritise identified topics/skills in the MERIT programme.

Results:

Differently from the first application of the methodology last year, now MERIT HEIs defined and submitted the syllabus of the master programs and course contents. We therefore grouped the learning outcomes of the programs and courses, comparing it with the envisaged set of skills of the first edition. The data relevant and/or used for Step 7 is written in italics.



MERIT graduates from VilniusTech, Taltech, RTU, and UPC are expected to be proficient in various domains. VilniusTech 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 behavior principles and understand the impact of proposed solutions*. Taltech program emphasizes the *design and optimization 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 financially *draft a business plan, 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, system design*, and understand the *legal and social aspects of system management*. UPC expects their 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 emphasize the importance of *continuous learning, ethical standards, teamworking, and the ability to propose innovative and sustainable solutions*.

Figure 2 reports a word cloud calculated on the learning outcome the syllabi of MERIT HEIs programs and courses. In both, artificial intelligence plays a prominent role.

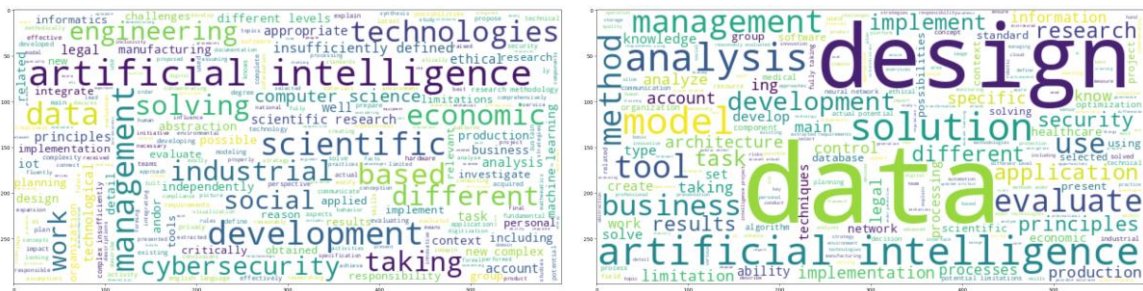


Figure 2: Word cloud generated from MERIT HEIs programs learning outcome (left) and courses learning outcome (right).

Compared with first-year expectations, MERIT HEIs have become more specific and tailored to the needs of the industry. However, the core competences such as fundamental knowledge, applied knowledge, and communication skills, 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.

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



Results:

Table 2 provides the agreed set of sources, the scope (Global, EU, or Regional), the domain (AI, CS, IoT), and whether they can be used to query research papers, statistics, reports or forecasts. We underline in the table the new set of sources (from the first-year edition) and cross those that were excluded (for instance, not having access or not being used as a source of reports anymore).

Table 2: List of data sources, their field and scope.

Source with link	Scope	Field	Used as a source of		
			Research or Statistics	Reports	Forecasts
ACM Digital Library	Global	AI/CS/IoT	V		
BASE - Bielefeld Academic Search Engine	<u>Global</u>	<u>AI/CS/IoT</u>	<u>V</u>		
Ebsco	<u>Global</u>	<u>AI/CS/IoT</u>	<u>V</u>		
Google Scholar	Global	AI/CS/IoT	V		
IEEEExplore	Global	AI/CS/IoT	V		
ResearchGate	Global	AI/CS/IoT	V		
Science Direct	Global	AI/CS/IoT	V	∅	∅
Scopus	<u>Global</u>	<u>AI/CS/IoT</u>	<u>V</u>		
Web of Science / Web of Knowledge	Global	AI/CS/IoT	V		
Wiley Online Library	<u>Global</u>	<u>AI/CS/IoT</u>	<u>V</u>		
Clusit	Regional (IT)	AI/CS/IoT	V	V	V
EC's AI Watch	<u>EU</u>	<u>AI</u>	<u>V</u>	<u>V</u>	<u>V</u>
ENISA	EU	AI/CS/IoT	V	V	V
EPoSS Association	EU	IoT	∅	V	∅
Forbes	<u>Global</u>	<u>AI/CS/IoT</u>			<u>V</u>
Frost & Sullivan	<u>Global</u>	<u>AI/CS/IoT</u>		<u>V</u>	<u>V</u>
Gartner	Global	AI/CS/IoT			V
Latvian Information and communications technology association	Regional (LV)	AI/CS/IoT	V		
OECD	<u>Global</u>	<u>AI/IoT</u>		<u>V</u>	<u>V</u>
IEEE Robotics & Automation society	Global	AI	V	V	
IBM	<u>Global</u>	<u>AI/CS/IoT</u>		<u>V</u>	
IEEE EAD	<u>Global</u>	<u>AI</u>		<u>V</u>	<u>V</u>
IEEE Innovation at Work	Global	AI/CS/IoT	V		
IoT Forum	Global	AI	V	V	
McKinsey & Company	<u>Global</u>	<u>AI/CS/IoT</u>		<u>V</u>	<u>V</u>
Splunk	<u>Global</u>	<u>CS</u>			<u>V</u>
World Economic Forum	<u>Global</u>	<u>AI/CS/IoT</u>		<u>V</u>	<u>V</u>
The REWIRE EU project	EU	CS	V	V	
Next Generation IoT	<u>EU</u>	<u>IoT</u>	<u>∅</u>	<u>∅</u>	<u>∅</u>



The second application of the methodology includes many new sources considering those reported in [2], which investigate reliable academic sources (ref. to parameter 1 in Table 4 of the study – which we filtered to search data in the context of the AI, CS and IoT) and which supports exact queries via quotes (parameter 18) to investigate specific keywords; then, available regional sources (mainly from MERIT partner regions) and the use AI-search engines (Microsoft Copilot and ChatGPT¹) to identify and discuss the inclusion of new ones.

Following is a list of new keywords used for the second edition:

- AI ethics / Responsible AI / AI governance;
- Cellular IoT;
- Data Ecosystems;
- Data Spaces;
- Digital Twins;
- Edge AI;
- Edge Analytics;
- Embedded Systems Engineer;
- Explainable AI;
- Intelligent Sensors;
- IoT Application Developer;
- IoT Data Analytics Expert;
- IoT Edge Application Platforms;
- IoT Marketplaces;
- IoT Network Engineer;
- IoT Platforms;
- IoT Product Manager;
- IoT Project Manager;
- IoT Security Platforms;
- IoT-based Streaming Analytics;
- LPWAN;
- MLOps;
- TinyML;
- Eorkforce framework AI / Cybersecurity / IoT.

In addition, we also employed this year the “site:” Google dork to restrict the search of specific keywords to the list of sources in Table 2.

Step 4) Analyse identified research papers, statistics, reports, and forecasts according to reported expertise.

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 2021), link, scope (Regional, European or Global), and a short summary of identified data. We underline all the data relevant and used in Step 4.

The McKinsey & Company *Technology Trends Outlook 2023* 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, Future of Mobility and Web3 all report (in order) the highest value of interest²; Applied AI, Advanced Connectivity and Future of Bioengineering instead rank (in order) among the top innovation values³. 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:

- Data science (M), machine learning (H) and TensorFlow (L) in the context of Applied AI - a trend **with a talent demand of 1:1 and maturity 4:5** in their investigation. Most requested job profiles: data scientist, followed by software engineer.

¹ Ref. to <https://copilot.microsoft.com> and <https://chat.openai.com> for additional details, respectively.

² 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 searches score is based on a measure of search engine queries.

³ As reported, 0 to 1 score for patents and research, which are relative to the trends studied. The patents score is based on a measure of patent filings, and the research score is based on a measure of research publications.



- Amazon web Services (L), continuous integration (M) and Cloud computing (M) in Next-generation software development⁴ - **talent demand 0.9:1**; maturity 2:5. Most requested profile is software engineer.
- Infrastructure management (H), Amazon Web services (L) and Cloud computing (M) in cloud and edge computing - **talent demand 0.7:1**; **maturity 4:5**. Most requested profile is software engineer.
- Risk analysis (M), regulatory compliance (L) and computer security (H) in Trust architectures and digital identity - **talent demand 0.55:1**; maturity 2:5. Most requested profile is security analyst, followed by software engineer.
- Maintenance (H) and automotive industry (M) and manufacturing (L) in future of mobility - talent demand 0.3:1; maturity 2:5. Most requested profile is software engineer.
- Photovoltaics (L) and contract management (M) in electrification and renewables; maturity 2:5.
- Regulatory compliance (H) and sustainability (L) in climate tech beyond Electrification and renewables; maturity 2:5.
- Kubernetes (L), IoT (M) and telecommunications (H) in Advanced connectivity - talent demand ~0.3:1; **maturity 4:5**. Most requested profile is software engineer.
- Product engineering (H) and computer vision (M) in immersive-reality technologies - talent demand 0.2:1; maturity 1:5. Most requested profile are software and mechanical engineer.
- pyTorch (L), machine learning (H) and Tensorflow (M) in industrializing machine learning - talent demand 0.4:1; maturity 2:5. Most requested profiles: data scientist, software engineer.
- Stakeholder management (L) and cloud computing (M) in Web3 - talent demand ~0.1:1; maturity 1:5. Most requested profile is software engineer.
- Pharmaceutical (L) and gene therapy (M) in future of bioengineering - talent demand ~0.2:1; **maturity 3:5**. Most requested profile is scientist.
- Aerospace industries (M) and aerospace engineering (L) in future of space technologies - talent demand 0.09:1; maturity 2:5. Most requested profile are software and system engineer.
- Regulatory compliance (L), Python (M) and machine learning (H) in generative AI - talent demand 0.05:1; maturity 1:5. Most requested profile is regulation affairs director, followed by data scientist.
- Cloud computing (L), Python (M) and Quantum computing (H) in quantum technologies - talent demand 0.02:1; maturity 0:5. Most requested profiles are scientist and software engineer.

In the context of **CyberSecurity (CS)**, the MERIT consortium highlights the following works:

- The 1st Annual cybersecurity Skills Trends report [3] from the Erasmus+ REWIRE project provides the current cybersecurity skill gaps⁵ and the most concerning cybersecurity threats to identify and anticipate future needs in the cybersecurity domain. It provides a comprehensive analysis which consider the output of a workshop to identify the cybersecurity, IT and soft skills in the context of NICE framework and taxonomy⁶ and of the European Cybersecurity Skill Framework (ECSF)⁷ – which we also considered in the first-year edition; an annual stakeholders' survey (138 responses from 21 EU countries in 2021); the developed Cybersecurity Job Ads Analyzer⁸ (358 ads considered in 2022, 927 in 2023); different pilot projects (Concordia, SPARTA, ECHO and CYBERSec4Europe) and threat reports (from ENISA, the, the Australian and UK cyber security centres); an annual review of sectoral surveys and studies (e.g., from ISACA, ISC and Fortinet) and the output of the REWIRE CyberAbility platform.

The highlighted set of competences to develop are:

⁴ Such as AI pair programmers; low- and no-code platforms; infrastructure as code; automated integration, deployment, and testing; and emerging generative-AI tools.

⁵ Defined by authors as the difference between the skills possessed by the workforce and those needed to function properly.

⁶ Ref. to <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center> for further details.

⁷ Ref. to <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsfc> for further details.

⁸ Available at <https://cyberability-platform.informacni-bezpecnost.cz/>.



Cybersecurity skills: Information Systems and Network Security; Business Continuity; Data Analysis; Data Privacy; Digital Forensics; Identity Management; Intelligence Analysis; Information Technology Assessment; Law, Policy, and Ethics; Testing and Evaluation; Physical Device Security; Risk Management; Incident Management; Data Security; Threat Analysis.

IT Skills: Data, Asset and Inventory Management; Database Administration; Enterprise Architecture; Network Management; Operating Systems; System Administration; Software Development.

Soft Skills: Communication; Organizational Awareness; Education and Training Delivery; Policy Development; Project Management; Strategic Relationship Management; Workforce Management (as soft skills).

Additionally, *Secure Development*, *Application security*, and *SecDevOps* were included considering the output of the stakeholders' survey.

Using the Job Ads Analyzer, at the time of writing the 10 most sought-after skills considering the available 937 positions are:

- Collaborate and Communicate (86.55 %);
- Information Systems and Network Security (65.85 %);
- Information Security Controls Assessment (59.45 %);
- Organizational Awareness (45.46%);
- Business Continuity (45.14 %);
- Threat Analysis (44.4 %);
- Data Security (43.86 %);
- Problem Solving and Critical Thinking (42.9%);
- Project Management (42.37%);
- Incident Management (41.73%).

Differently from the second edition of the report [4], Risk Management decreased from ~49% to ~41%; Enterprise Architecture and Infrastructure Design from ~45% to ~41%; Organizational Awareness decreased ~3%, while Incident Management ~5%. Differently from the first edition, the list now does not include Network Management (currently ~26%); Software Development (~20%); Operating Systems (~35%); Policy Development (~36%); Law, Policy, and Ethics (~31%); Database Administration (~11%); Education and Training Delivery (~17%) and Strategic Relationship Management (~36%).

When mapping the job ads requirements to the European Cybersecurity Skill Framework (ECSF), in the first edition of the report 50.28% requested the Cybersecurity Implementer profile and, more specifically, the Cyber Security Engineer and Cyber Security Specialist roles: i.e., a figure which develop, deploy and operate cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products [5]. No ads requested the skills/knowledge of the Cybersecurity Educator profile. In the second edition of the report [4], the Cybersecurity Implementer remains the top-most requested profile (with 148 related job ads), followed by the Cybersecurity Architect (142 ads) and the Incident Responder (115). In the second edition, 18 ads are in relation to the Cybersecurity Educator.

From the Concordia pilot, authors report in the first edition the following topics of interest: big data, internet-of-things, and artificial intelligence, followed by mobile devices and cloud computing. They also highlight the link between the industry and the requested working knowledge and skills.

From the SPARTA project, they report the set of challenges expected to be more relevant in future: Autonomous Security for Self-Protected Systems; Trustworthy Software; Quantum Information Technology; 5G Security; Next-generation computing architectures.

From the CyberSec4Europe, the most demanded cybersecurity skills are, in order: Personal Data Protection and Privacy, Secure Communication Protocols, Data Integrity and Authentication, Data Privacy and Access Control. The most demanded job profiles are: Digital Forensic Analyst; Chief Information Security Officer; Security Operations Centre Manager; Information Security Officer and Software Engineer. The most demanded skill categories over all profiles are Human Security, Data Security, Societal Security, Connection Security and Organizational Security. When requesting companies the importance of each skill for a job profile, CyberSec4Europe collected five skills (4 of which were in the Data Security category): Personal Data Protection and Privacy; Secure Communication Protocols; Data Integrity and Authentication; Data Privacy; Access Control.



The report discusses also the threats identified by the ENISA Threat Landscape 2022, which are addressed again in the second edition of the report (being confirmed by the ENISA Threat Landscape 2023). They are (in order of importance) ransomware, malware, social engineering, threats against data, threats against availability and integrity, disinformation/misinformation, and supply-chain attacks. In the context MERIT programs and activities those could be explored more to better protect future employees and their organizations, as the human factor plays a crucial role (for instance, supporting user awareness programs to counter possible attacks leveraging phishing and social engineering). The second edition of the report also maps the beforementioned threats to the cybersecurity skills that could be employed by each of the 12 ECSF profiles to address them (based on best practices and practical expertise). Each skill is weighted from 1 to 5 (being of utmost importance in countering the threat).

Those reported for the Cybersecurity Implementer profile are:

- [in the context of the reported Operation Technology threats] communicate, present and report to relevant stakeholders; and develop code, scripts and programmes.
- [with Information Technology threats] conduct network configuration and setup.
- [with Shared Information Technology Threats] develop code, scripts and programmes; communicate, present and report to relevant stakeholders; performs basic risk assessments for small information systems; assess the security and performance of solutions; conduct network configuration and setup; contribute to the identification of risks that arise from potential technical solution architectures; suggest alternate solutions or countermeasures to mitigate risks; define secure systems configurations in compliance with intended architectures.

For the Cybersecurity Architect:

- [Operation Technology threats] define, present and promote an information security policy for approval by the senior management of the organization; coordinate the integration of security solutions; monitor progress of issues throughout lifecycle and communicate effectively; contribute to the development of ICT strategy and policy, including ICT security and quality; plan and implement application and data provisioning; guide and communicate with implementers and IT/OT personnel.
- [Information Technology threats] monitor progress of issues throughout lifecycle and communicate effectively; plan and implement application and data provisioning; dealing with problems; contribute to the development of ICT strategy and policy, including ICT security and quality; conduct performance and resilience testing; plan and implement application and data provisioning.
- [Shared Information Technology Threats] coordinate the integration of security solutions; monitor progress of issues throughout lifecycle and communicate effectively; conduct performance and resilience testing.

For the Incident Responder profile:

- [Operation Technology threats] recognize and categorize types of vulnerabilities and associated attacks; secure network communications; manage and analyse log files; collect, analyse and correlate cyber threat information originating from multiple sources; work on operating systems, servers, clouds and relevant infrastructures.
- [Information Technology threats] protect a network against malware (e.g., NIPS, anti malware, re strict/prevent external devices, spam filters); secure network communications; collect, analyse and correlate cyber threat information originating from multiple sources; recognize and categorize types of vulnerabilities and associated attacks.
- [Shared Information Technology Threats] recognize and categorize types of vulnerabilities and associated attacks; collect, analyze and correlate cyber threat information originating from multiple sources; manage and analyze log files; work on operating systems, servers, clouds and relevant infrastructures.



- In [6] ENISA provides a methodology to identify and prioritize (via likelihood, impact and novelty) 21 cybersecurity threats for EU infrastructure and services (to emerge or be exacerbated by the year 2030). For each threat, it indicates the probable actors (among state-sponsored, cybercrime, hackers-for-hire, and hacktivists), methods, impact, plausible future scenarios⁹, topics for future Single Programming Document (SPD), relevant ENISA strategic objectives and an attack example. Following is the list of the top 10 (future) cybersecurity threats.
 1. Supply chain compromise of software dependencies;
 2. Advanced disinformation and influence operation campaigns;
 3. Rise of digital surveillance authoritarianism and loss of privacy;
 4. Human error and exploited legacy systems within cyber-physical ecosystems;
 5. Targeted attacks (e.g., ransomware) enhanced by smart device data;
 6. Lack of analysis and control of space-based infrastructure and objects;
 7. Rise of advanced hybrid threats;
 8. Skills shortage;
 9. Cross-border ICT service providers as a single point of failure;
 10. Artificial intelligence abuse.

The document highlights the following 6 future technology trends:

1. Increasing popularity of everything as a service (XaaS) demand and supply (and in particular cloud computing and IoT sensors);
2. Satellite control infrastructure being increasingly critical;
3. AI-based systems increasingly deployed with bias or issues that impact inclusivity, safety, ethics, privacy, trustworthiness, and explainability;
4. Extended Reality going mainstream;
5. Vehicles becoming increasingly connected to each other and to the outside world, and less reliant on human operation;
6. Digital Twins entering the mainstream use (more accessible to organizations large and small, across industries).

The document also indicates among the future economic trends the use of distributed ledger technologies, user-behaviour analysis (especially in the private sector) and the rise of smart cities and the Web3: the third iteration of the internet and will be defined by open-source technology, utilizing blockchain technology to be trustless and permissionless.

In [7] Clusit indicates malware as the top attack vector globally¹⁰ in the first six months of 2023 (35.7% of successful attacks, -1.3% with respect to 2022), followed by unknown techniques (21% of incidents reported without providing further details, -3% w.r.t. 2022), known vulnerabilities and zero-days (16.8%, +4.8% w.r.t. 2022), phishing and social engineering (8.6%, -3.4% w.r.t. 2022), DDoS (7.9%, +3.8 w.r.t. 2022) and “sophisticated attacks” (8%, -1.4% w.r.t. 2022); Identity Theft and Account Hacking is at 3.3% (+0.3 w.r.t. 2022). In Italy, malware (31%) is followed by DDoS at 30%. The focus sections highlight the following:

- How predictive algorithms and a risk-based approach can help manage vulnerabilities in complex systems, using the Known Exploited Vulnerabilities (KEV) catalog from the US Cybersecurity and Infrastructure Security Agency (CISA).

⁹ 1. Blockchain, deepfakes, & cybercrime in a data-rich environment; 2. Eco-friendly, sustainable, and interconnected smart cities (non-state actors); 3. massive data collection with less control; 4. Sustainable energy, automated/short-term workforce; 5. (highly regulated) legislations, bias, extinctions, & global threats.

¹⁰ Using a database of more than 17,000 incidents classified by severity, types of attackers and victims, technique, and geographic area.



- The features and benefits of a next generation SOC, which integrates advanced technologies such as artificial intelligence, automation, orchestration, and threat intelligence to improve the detection and response capabilities of security teams.
- The new attack vectors that emerge from the development of smart mobility solutions, such as APIs and recharge lines, and the challenges they pose for the security of connected vehicles and infrastructures.
- The benefits of the cyber threat intelligence, which is the process of collecting, analyzing, and disseminating information about current and emerging cyber threats, to support security decision making and operations.
- The potential and challenges of Artificial Intelligence (AI), data, and cybersecurity, and how they can interact in a positive or negative way.

In [8] authors discuss the use of competency models in the information security and cybersecurity domains. They review 27 models and extract 240 competencies (most of them in the “professional” category – in line with assessed models), and complement the study with additional competency classes: the results is based on CyBOK¹¹ and considers 19 Knowledge Areas (KAs). The 3 most frequent KAs among models are:

1. Security operations and incident management;
2. Risk management and governance;
3. Secure software lifecycle.

The human factor follows as the fourth KA.

In the healthcare sector, which remains one of the sectors most affected by cybercriminals, authors of [9] identifies the top 12 most critical areas of cybersecurity knowledge: Risk Management; Cybersecurity Principles and Management; Cybersecurity in Practice for Health Sector; Privacy and Data Security; Security Operations (SOC); Cybersecurity Policies and Procedures; Cybersecurity Incident Response; Cybersecurity Awareness and Training; Systems Security; Penetration Testing; Cybersecurity Audit; Cybersecurity Law and Compliance.

In [10] authors highlight the current central role of CISOs as strategists and leader, participating in board level committees and growing their influence within corporate power centers. Their study¹² administered a quantitative survey to 350 CISOs, CSOs and other qualified executive security leader equivalents between North America, EMEA, and APAC; and a qualitative investigation through pone interviews targeting 20 CISOs, CSO and security leaders from US, Canada and UK. The most important findings are:

- The use of generative AI, from mundane technical tasks (e.g., internal communication) to filling cyber defense gaps: to analyze data sources to reduce false positives, for malware analysis, to create policies, detection rules and secure configurations, for threat hunting, workflow automation, risk scoring, and incident response and forensics investigation.
- The most concerning cyber threats for interviewed CISOs are social engineering, operational technology (OT) and Internet of Things (IoT) threats, ransomware (which affected many of the interviewed organizations).

¹¹ Ref. to <https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf> for additional details.

¹² 17 industries involved, including financial services (banking, securities, insurance), manufacturing, media and communications, technology, healthcare, retail/wholesale, business services, government/public sector, education (K-12, secondary, college/university), agriculture/forestry, construction/engineering, consumer packaged goods, life sciences, mining/oil/gas, telecom, transportation, utilities.



- Cloud applications and infrastructure are indicated as having the biggest security gaps by CISOs in business service, healthcare, technologies and manufacturing. Financial services CISOs indicate instead the third party/supply chain security as the one to prioritize.

Summarizing reported data, the current and forecasted topics/skills for CS are:

- AI-based cybersecurity systems;
- Application security;
- Authentication and Access Control;
- Automotive security;
- Business continuity;
- Cloud applications and infrastructure;
- CVEs;
- Cyber threat intelligence;
- Cybersecurity Audit;
- Cybersecurity Awareness and Training;
- Data analysis;
- Data integrity;
- Data privacy;
- Develop code, scripts and programs;
- Digital Forensics;
- Digital Twins;
- Everything as a service;
- Extended Reality;
- Human-factor in security;
- Identity management;
- Incident management;
- Information security controls assessment;
- Information systems;
- Intelligence analysis;
- IT assessment;
- Law and compliance;
- Network configuration and setup;
- Next generation SOC;
- Organizational Security;
- Penetration Testing;
- Personal data protection;
- Physical device security;
- Predictive algorithms;
- Risk assessments;
- Risk Management and governance;
- Satellite control;
- Secdevops;
- Secure communication protocols;
- Secure development;
- Secure software lifecycle;
- Smart mobility solutions;
- Societal security;
- System, network and data security.
- Testing and evaluation;
- Threat Analysis.

In addition, mechanisms to protect against ransomware, malware, social engineering, DDoS, phishing and social engineering, operational technology (OT) and Internet of Things (IoT) threats; threats leveraging disinformation/misinformation, and supply-chain attacks.

In the context of **IoT**, the MERIT consortium highlights the following works:

- In [11] authors investigate the existing strategic themes, thematic evolution structure, key challenges, and potential research opportunities associated with the IoT. For this study, a Bibliometric Performance and Network Analysis (BPNA) has been conducted, supplemented by an exhaustive Systematic Literature Review (SLR). Specifically, in BPNA, the software SciMAT has been used to analyze 14,385 documents and 30,381 keywords in the Web of Science (WoS) database, which was released between 2002 and 2019. The results reveal that 31 clusters are classified according to their importance and development, and the conceptual structures of key clusters are presented, along with their performance analysis and the relationship with other subthemes. The thematic evolution structure describes the important cluster(s) over time. For the SLR, 23 documents have been analysed. The SLR reveals key challenges and limitations associated with the IoT. The results could form the basis of future research and guide decision-making in the IoT and other supporting industries. Findings that emerged from the analysis reveal that main patterns related to IoT are:



- **Authentication:** authentication methods can be seen as a series of adopted procedures to confirm an entity's identity in a network. In the IoT environment, security and privacy are the primary concerns. Since the equipment does not have many resources to protect, data leakage is hindered, which makes it very difficult to attack robust security systems.
 - **6LOWPAN:** Low-Power Personal Area Networks refer to devices with low energy consumption, computer power consumption and memory. They communicate using low-power wireless standards.
 - **Industry 4.0:** this concept of building a new economy based on high-tech technologies accelerated the fourth industrial revolution and is based on technologies such as cyber-physical systems, IoT, big data and analytics, cloud computing, sensors, machine learning, computer simulation, 3D printing, artificial intelligence, augmented reality, real-time monitoring and decision-making, cybersecurity, robotics, among others.
 - **Smart city:** this concept can be seen as using the IoT and other emerging technologies to improve the functions of cities. IoT can be applied in heterogeneous environments and is the best way to improve smart cities.
 - **Cloud Computing:** cloud computing uses Internet protocols as a model for consumption and delivery of technology resources. This technology is characterized by on-demand accessibility of systems, large data storage and high computer capacity.
 - **Machine Learning:** machine learning algorithms are used to learn from data, make sense of data, and discover patterns that can be used to predict what will happen in future situations. Recently, the interest in using machine learning to improve IoT security is increasing.
 - **Distributed System:** a distributed system is a group of autonomous computers presented to its users as a single integrated system. Important roles of distributed systems are storage, collaborative computing, and security.
 - **Interoperability:** interoperability is a property of a system that shares data and communicates with other systems.
 - **Platforms:** a platform facilitates exchanges, reduces transactions cost, facilitates transactions between companies and provide products and services. IoT platforms integrate tasks into information and provides services for IoT devices through cooperation with other platforms.
 - **SOA (Service Oriented Architecture):** SOA is a software architecture that allows the connection of resources to get or give data on demand. It enables interoperability between various IoT devices.
- In [12] authors provide a systematic review of the existing literature on IoT adoption in organizations via five electronic databases from 2015 to July 2021. Seventy-seven articles have met the eligibility criteria and were analysed to answer the research questions. This study produced a coherent taxonomy that can serve as a framework for future research on IoT adoption in organizations. It highlights an overview of the essential features of this emerging technology in terms of IoT adoption benefits and challenges in organizations. Existing theoretical models have been analysed to identify the factors that influence IoT adoption and to understand the future requirements for widespread IoT adoption in organizations. Six critical factors affecting and playing a key role in IoT adoption in organizations were identified based on the critical review findings: technological, organizational, environmental, human, benefit, and value. Decision-makers and developers can prioritize these critical factors and progressively improve their development to enhance IoT adoption efficiency. The reported factors that influence the IoT adoption in organizations are:
 - **Technological factor:** relative advantage, complexity, compatibility, security and privacy, IT infrastructure, implementation cost, technology readiness, perceived usefulness, perceived ease of use.
 - **Organizational factor:** organizational readiness, absorptive capacity, top management support, innovation capacity, organization sector, organization size, organization age.



- Environmental factor: competitive/external pressure, government regulations, environmental uncertainty, vendor/outside support.
 - Human factor: IT skill and knowledge, IT expertise, employee resistance, customer experience, trust.
 - Benefit factor: perceived benefits, business integration, customer satisfaction, tasks efficiency, better decision making, data accuracy and analytics, competitive advantages, new revenue stream, asset management efficiency.
 - Value factor: business value, timesaving, cost optimization.
- In [13] the author performs an extensive literature review (2768 unique publications via bibliometrics on Scopus and WoS core collections) to identify the scientific IoT trends overtime in 8 areas: IoT applications, types, security, data, communication networks, development, protocol standards, and technologies. Following are the main findings of the three categories with most interest in literature:
 - IoT applications (the 47.86%, of the total IoT works under review) prioritize energy, industrial and healthcare applications, the integration of IoT with Cloud Computing, and the pollution sectors. Then, smart home and smart grids.
 - IoT technologies: application protocols works highlight DDS, COAP, AMQP, MQTT, MQTT-SN, XMPP, and HTTP REST; service discovery protocols highlight Multicast DNS, and DNS-SD; infrastructure protocols include routing protocol (RPL), network layer (6LowPAN, IPv4, IPv6), link layer (IEEE 802.15.4), physical/device Layer (LTE-A, EPCglobal, Z-Wave); Other protocols mentioned among reviewed works are IEEE 1888.3, IPSec, IEEE 1905.
 - IoT security (21.3%) prioritise data security, big data issues, authentication, access control, anonymity, privacy, and confidentiality. Protection against malware and cybercrime are also mentioned. The security issues extracted include IoT platform, IoT solutions based on blockchain and cloud, edge and fog computing; IoT networks, lightweights and cryptography (encryption). The security of IoT platforms such as Amazon, ARM, Azure, and Microsoft is also mentioned.

Summarizing reported data, the current and forecasted topics/skills are strongly influenced by the innovation introduced by artificial intelligence and the improvement of technologies, which brings with it an improvement in the security posture. A possible list includes:

- Authentication and Access Control, and more general cybersecurity measures;
- Application layer protocols (such as DDS, COAP, AMQP, MQTT, MQTT-SN, XMPP, COAP);
- Routing protocols (e.g., 6LOWPAN);
- Physical/device layer protocols (LTE-A, EPCglobal, Z-Wave);
- Cyber-physical systems;
- Big data and analytics;
- Cloud, edge, and fog computing;
- Computer simulation;
- Robotics;
- Use of 3D printing in IoT;
- Machine learning and artificial intelligence (e.g., to obtain advanced insights or for decision-making);
- Augmented reality;
- Real-time monitoring;
- Distributed System;
- IoT platforms (e.g., Azure or AWS);
- Service-oriented applications (SOA);
- 5G and device connectivity;
- Smart cars and Smart cities, smart homes and smart grids applications;
- The use of IoT in energy, industry and healthcare scenarios.



In the context of **AI**, the MERIT consortium highlights the following Works:

- In [14] authors investigate the use and potential threats of Artificially Intelligence (AI) technologies (including generative AI tools) in workplaces. The assessment includes five inductively generated themes within a multilevel framework: (i) human–AI collaboration (to complement or augment human work, skills or training); (ii) perceptions of algorithmic and human capabilities (particularly, whether to accept AI for certain tasks or rely on AI-provided advices); (iii) worker attitudes towards AI (and the different fear they face – e.g., replace their task or introduce new skills); (iv) AI as a control mechanism in algorithmic management of platform-based work (and more generally how AI technologies transform the labour market); and (v) labour market implications of AI use.
- In [15] authors highlight how Artificial Intelligence (AI) implementations have unique characteristics, such as dealing with probabilistic outputs. To address these challenges, the authors conducted 25 explorative interviews with experts from industry, consulting, and academia, derived four organizational capabilities and propose an explanatory framework of how these capabilities facilitate AI implementation. The four capabilities are:
 1. AI Project Planning (identify, evaluate and prioritize sustainable AI use cases).
 2. Co-development of AI systems (communicate with and integrate stakeholders in AI implementation).
 3. Data Management (collect, curate, and provide data for AI implementation)
 4. AI Model Lifecycle Management (orchestrate the evolution of AI models, including development, deployment and maintenance).
- In [16] authors investigate the competencies needed to leverage AI effectively by adopting a hybrid approach. First, they conduct a qualitative content analysis of the practical and scientific literature to derive and structure the existing body of knowledge (from EBSCOhost, Scopus and Wiley Online Library). Subsequently they perform a quantitative content analysis of 9,247 job advertisements (from the job platform Indeed, from 60 countries using the tool Octoparse). The results integrate the key technical and managerial competencies from both literature and market demand.
 - Technical competencies: knowledge in AI-associated technologies and algorithms (ML, deep learning, neural networks), programming (Python, Scala, Java, web development), AI frameworks and libraries (TensorFlow, Pytorch, Keras, Scikit-learn, Numpy, Caffe), big data analytics frameworks (Spark, Hadoop); STEM knowledge (mathematical and statistical knowledge, computer science); development methodologies (Agile software development); problem solving (initiative/engagement); data management (data management).
 - Managerial competencies: business management (client focus/orientation, decision making); business acumen (business development, interdisciplinary knowledge); people and social skills (collaboration, building trust, leadership); communication (oral and written communication).

Their analysis highlight also how AI-related competencies are highly significant in the labour market, especially in the identified three job cluster (Data Science and Engineering, Software Engineering and Development, and Business Development and Sales); and that there is no explicit demand in the labour market for a workforce utilising AI on an operational level (to be instead they are sought along the development process).

- In [17] authors develop a conceptual research model that explores the effect that AI competencies have on B2B marketing and test it via 155 survey responses from senior IT executives in the Nordic EU countries (and hypothesized relationships by using a PLS-SEM approach). The result is that organizations that can foster AI competencies will achieve organizational performance gains through their B2B operations in three channels: information management, planning, and implementation.



- The review in [18] provides a rigorous overview of the state of the art based on 107 records published across the fields of human-computer interaction, learning sciences, computing education, and child-computer interaction between 2010 and 2020. The findings show the urgent need on a global scale for inter- and transdisciplinary research that can integrate these dispersed contributions into a more coherent field of research and practice. Nine discussion points are provided for developing a shared agenda to mature the field. Based on the HCI community's expertise in human-centred approaches to technology and aspects of learning, we argue that the community is ideally positioned to take a leading role in the realisation of this future research agenda. Keywords: K–12 education, emerging technologies, computing education, computational literacy.
- In [19] authors provide a comprehensive systematic literature review (SLR – via co-citation analysis, bibliographic coupling, co-word analysis) on the intersection of artificial intelligence (AI) and innovation research. It includes an analysis of 1448 articles from databases like Web of Science and Scopus. The review identifies economic, technological (Big data, IoT, Digital platforms), and social (Sustainability, waste management) factors as drivers of AI adoption in firms for innovation, as well as the outcomes of such adoption. It also develops a conceptual framework and proposes a research agenda with over 70 questions for future studies. It concludes with a bibliometric analysis highlighting the dominant topics, key publications, and trends over time.
- In [20] authors offer a systematisation of the competencies and skills for AI, highlighting the most prominent (data science, firm performance), basic (artificial intelligence, future and innovation), specialised (self-efficacy, competence and outcomes), and emerging (analytics) themes in the period 2016 to 2020, and providing a performance measure analysis of this field. In addition, major challenges and a research agenda are discussed. The organisational challenge is to achieve a workforce with the necessary digital competencies, and to adapt human resource management practices to AI challenges.
- In [21] authors presented a systematic review study that aims to understand the opportunities and challenges of AI application in higher education (AIEd) by examining the literature from the last 10 years (2012–2021) from ERIC, ProQuest, Scopus, and WOS and using matrix coding and content analysis approaches. The results present the current focus of AIEd research by identifying 13 roles of AI technologies (from assigning tasks to automatic marking and predicting performance) in 4 key educational domains (learning, teaching, assessment, and administration), 7 learning outcomes of AIEd, and 10 major challenges. The review also provides suggestions for future directions of AIEd research.
- In [22] authors provide a comprehensive analysis of the use of AIEd from 2016 to 2022. It highlights a significant increase in publications, particularly in 2021 and 2022, and a geographical shift, with China surpassing the US in the number of publications. Interestingly, the document notes a trend of researchers from departments of education becoming the most dominant contributors to this body of literature. The document further reveals that most studies (72%) focused on undergraduate students. Language learning emerged as the most common subject domain (followed by computer science and engineering) where AIE was applied. The reported five applications of AIEd are: (i) Assessment/Evaluation, (ii) Predicting, (iii) AI Assistant, (iv) Intelligent Tutoring System (ITS), and (v) Managing Student Learning.
- In [23] ENISA explores the dual-use nature of AI: to enhance cybersecurity as well as to launch cyberattacks. Then, it identifies the main challenges and opportunities in this field. The document presents a hybrid approach and gives some suggestion to develop a secure AI system from malicious manipulation, adversarial attacks, and ethical issues, and provides some examples of AI use cases in domains such as telecommunications, IoT, CPS, and biosecurity. The document identifies five research needs for AI and cybersecurity, which are: (1) developing trustworthy, reliable, and explainable AI; (2) improving the quality and availability of data sets for AI; (3) designing end-to-end protection mechanisms for AI; (4) developing standardised frameworks and testbeds for AI; and (5) exploring the potential of AI-powered penetration testing.



Summarizing reported data, the current and forecasted topics/skills for AI are:

- Generative AI tools;
- Chats boots;
- Large Language Models (LLM);
- Cyber AI;
- Data science;
- AI and the future of education;
- AI and Marketing;
- Human-AI collaboration;
- Effects of AI in workplaces;
- Effect of AI on social and occupational wellbeing;
- Secure AI systems;
- Adversarial attacks;
- Ethical issues;
- Improving the quality and availability of data sets for AI;
- Explainable AI;
- Artificial Intelligence (AI) in higher education (such as teaching in the AI era);
- AI Project Planning and Co-Development;
- Role of AI in software;
- Developing standardized frameworks and testbeds for AI;
- Machine learning;
- TensorFlow.

As part of the data under review (AI, CS, and IoT), we were able to also extract the following set of soft skills: collaborate and communicate, present and report to relevant stakeholders; project management; work ethically; have organizational awareness and foster workforce management; deliver education and training; strategic relationship management; problem solving and critical thinking.

Step 5) Request partner SMEs to highlight their needs and, together with DIHs, inquire regional market needs administering a questionnaire in their network. In the following results, we provide the number of organisations participating the questionnaire, the field in which they operate 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 first edition of the methodology.

Cybersecurity questionnaires discussion:

The cybersecurity questionnaire was replied by 10 organisations operating in the cybersecurity area or different domains: one in fintech, one in robotics, AI and IoT; one in marketing; others offering more general IT services. The results we want to highlight are:

- 4/10 are currently leveraging (i) machine learning with context-awareness, (ii) human-computer-Interaction, (iii) monitoring of large-scale and possibly interconnected systems, and (iv) techniques to prevent ransomware and a SOC as-a-Service as part of their daily operations; 4 intend to do so with machine learning with context-awareness in future. Considering the technologies, the same number adopt: (i) Just-in-Time (JIT) access and Just-Enough Access (JEA) administrator access, (ii) privilege separation and least-privileged access, as well as using Privileged Access Workstations (PAWs) for managing identity systems, (iii) smart mobile app, (iv) DevSecOps, (v) intelligent automated sorting, (vi) API management PaaS, (vii) distributed cloud systems, (viii) hybrid cloud storage, (ix) Network Detection and Response (NDR), (x) Security Orchestration Automation and Response (SOAR), (xi) Zero Trust principles (Zero Trust Network Access - ZTNA).
- 5/10 leverage decision intelligence and techniques to prevent OS vulnerabilities. For technologies: (i) Extensive detection and response (XDR), (ii) automation of preventive measures, and encrypting personal and sensitive data, (iii) proactive threat detection, (iv) AI cloud services and AIOps, (v) Endpoint Detection and Response (EDR), (vi) identity-based security technologies, (vii) identity-based segmentation, (viii) SD-WAN and Network Traffic Analysis, (ix) Managed Detection & Response (MDR), (x) Operation Control Centre (OCC), (xi) Security information and Event Management (SIEM).



- 6/10 adopt the SaaS business model and phishing prevention techniques. For technologies, they declare adopting Multi-Factor-Authentication (MFA) or Conditional Access Control.
- 7/10 leverage predictive analytics and user behavioral tracking.

Those results demonstrate that the list provided in the first-year edition (D3.1) includes a substantial number of skills and technologies currently leveraged (37/52).

No organisation is currently leveraging the expertise with biomimetic cybersecurity algorithms and cyber biosecurity, but two plan to do it in future. For technologies, Blockchain and Citizen Integrator Tools are not adopted currently or in the following two years (except in one case, for Blockchain, between one and two years). This could demonstrate the possible future skill needs, but a larger sample of organisation should be investigated to support this claim.

It is worth noting that one of the organisations strongly suggested considering also Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Run-time Application Security Protection (RASP), Interactive Application Security Testing (IAST), Vulnerability management for DevSecOps, Threat Modelling, the use of AI for vulnerabilities and generative AI awareness.

The CS questionnaire and the last year D3.1 investigation share 25 areas and technologies: human-computer-Interaction; monitoring of large-scale and possibly interconnected systems; OS vulnerabilities; privilege separation and least-privileged access, as well as using privileged access workstations (PAWs) for managing identity systems; Just-in-Time (JIT) access and Just-Enough Access (JEA) administrator access; Extensive detection and response (XDR); Zero Trust principles (Zero Trust Network Access - ZTNA); SOAR; Endpoint Detection and Response (EDR); managed Detection & Response (MDR); Network Detection and Response (NDR); Phishing and Ransomware prevention; MFA or Conditional Access Control; Operation Control Centre (OCC); distributed cloud systems; hybrid Cloud Storage; identity-based segmentation, SD-WAN and Network Traffic Analysis; AI cloud services and AIOps; API management PaaS; SOC as a Service; SIEM; Identity-based security technologies; SaaS business model; predictive analytics; user behavioural tracking; proactive threat detection; automated incident response protocols and automation of preventive measures and encrypting personal and sensitive data. Differently from D3.1 results, now organisations indicated an interest in decision Intelligence; smart mobile app; devSecOps and intelligent automated sorting.

Artificial Intelligence questionnaires discussion:

The AI questionnaire was replied by 13 organisations operating in the AI-related domains, from fintech to accounting systems and telecommunication, robotics, teaching, cybersecurity and marketing; others offer more general IT services. The results we want to highlight are:

- 6/13 adopt AI for (i) algorithm designing, (ii) product marketing, (iii) business management, (iv) technology design and programming.
- 7/13 are currently leveraging (i) data processing and management and (ii) knowledge representation and reasoning, planning, search, and optimization as part of their daily operations. Considering the technologies, the same number adopt: (i) big data, (ii) digital marketing, (iii) critical thinking and analysis, (iv) complex problem solving, (v) active learning and adoption of new technology, (vi) analytical thinking and innovation.
- 8/13 adopt (i) machine learning technologies and (ii) AI tools and technology for reasoning, problem-solving and ideation.
- 9/13 employ AI with cloud technologies.



Differently from the cybersecurity output, here the majority only leverage 2 of the 19 inquired expertise, while at least one organisation adopts each requested technology¹³. In addition, no organisation declares to currently leverage AI in smart manufacturing (2 will do it in future), AI adoption index (1 will do it next year and 4 in future), AI in retail industries (6 will do it in future), AI in agriculture (3 will do it in future), Autonomous driving (4 will do it in future), AI in space industries or more generally spatial data processing (1 will do it next year and 2 in future).

Those results can be linked with the specificity of the domain in which the enterprises operate, but they still open a window of opportunity over the possible skills required in the future.

In both applications of the methodology, with respect to the Artificial Intelligence domain, machine learning plays a pivotal role (considering D3.1 “use of ML to boost resiliency”), together with data management (D3.1 reported “data management via databases”). Differently from D3.1, the questionnaire highlights the interest of organisations in knowledge representation and reasoning; big data; algorithm designing; product and digital marketing, and business management; technology design and programming; cloud technologies and more general skills in the AI context: critical thinking and analysis, complex problem solving, active learning and adoption of new technology, analytical thinking and innovation.

In future interactions, it would be of interest to also request organisations their interest in some of the AI applications that could not find place in the (already extensive) questionnaire: the use of AI with data mining; ML with context awareness; intelligent Object Recognition; the use of cloud-native tools that use machine learning to separate noise from signals; software to optimize routes, time and costs (or to reduce emissions); asset health monitoring and management, or predictive maintenance, automated preventive measures and disruption management; predictive analytics and Operation Control Centre (OCC); Self-service technologies; Biometric verification, touchless ID, MFA and Access Control; user behavioural tracking (in line with the new AI act); proactive threat detection and automated incident response (e.g., to support eXtensive Detection and Response - XDR); Image processing algorithms; Multi-parameter sensing; Error detection; Secure & Autonomous Communication; the SaaS business model; auto-steer and manoeuvrability; prediction of traffic conditions.

Internet of Things questionnaires discussion:

The IoT questionnaire was replied by 8 organisations operating in the IoT domain or different ones: software development, marketing, robotics, or more general IT services. The majority of organisations declare smart environment applications (e.g., measure level of water and flow, air quality monitoring - 5/8 organisations), those associated with smart home (e.g., water leak detector, smart lighting - 6/8 ones), smart transportation (e.g., traffic management, parking management, billboard monitoring - 6/8) and smart industry (e.g., product management, energy saving, product tracking - 7/8) to be deployed in their region. In addition:

- 4/8 organisations indicate smart home and smart transportation applications will (continue) to be deployed in their region within one year; similarly, smart cities technologies later in future. One organisation suggests considering the use of sensors for monitoring students' behavior and to support personalized learning.
- When requesting the IoT technologies, the majority currently adopts digital twins (4/8 organisations), intelligent sensors (5/8) and cellular IoT (2G/3G/4G/5G - 7/8). 4/8 organisations will adopt (in the context of IoT) blockchain¹⁴, data ecosystems or data spaces and more generic IoT platforms; 5/8 edge analytics and TinyML.

¹³ Two organisations adopt 2 other technologies, and five the remaining 8 technologies not reported in the list.

¹⁴ It is worth mentioning that the remaining 4 other organisations have no plans to adopt it.



Similar considerations to the AI questionnaire responses also apply to IoT ones (specific domain / window of opportunities).

The interest of organisations from the IoT questionnaire focuses on digital twins and intelligent sensors; and ranges across different sectors, such as environment, home, industry, and transportation.

With due time, it will be important in future interactions to request local SMEs operating in the IoT sector about their interest in specific applications (e.g., asset health monitoring and management, AI-supported recycling robots, software to optimize resource consumption, and 5G/6G services) but also the underlying technologies (e.g., blockchain for IoT device firmware, communication networks and technologies, machine learning applied to IoT, data analytics), security aspects (e.g., IoT devices in Zero-Trust networks), and business models (e.g., SaaS, Economy of Things and Data Brokerage).

Step 6) Generate a summary of required AI, CS and IoT technologies and skills/topics by considering both the state-of-the-art data (Step 4) and industrial needs (Step 5).

Results

The following set reports the **CS** topics and technologies which were indicated by at least half of the organisations via the questionnaire in Step 5, and are in the context of the data extracted from research papers, statistics, reports, and forecasts from Step 4¹⁵:

- Monitoring of large-scale and possibly interconnected systems;
- Machine learning with context-awareness;
- Decision Intelligence;
- Automation of preventive measures, and encrypting personal and sensitive data;
- Predictive analytics;
- Threat Modelling;
- DevSecOps;
- Phishing (prevention);
- Zero Trust principles (Zero Trust Network Access - ZTNA);
- AI cloud services and AIOps;
- Ransomware (prevention);
- User behavioural tracking;
- Cloud-native tools that use machine learning to filter logs;
- Proactive threat detection;
- Automated incident response protocols;
- Security information and Event Management (SIEM);
- Vulnerability management for DevSecOps;
- OS vulnerabilities;
- The use of AI to detect vulnerabilities;
- Privilege separation and least-privileged access, as well as using privileged access workstations (PAWs) for managing identity systems;
- Identity-based segmentation, SD-WAN and Network Traffic Analysis.

Compared with the list of topics and skills from the first-year edition, the current one focus more on CS concepts (e.g., it excludes IoT security, cybersecurity laws and regulations, AI-based data processing and cloud localisation risks¹⁶), with less attention to operational technology and risk management, but more on the secure development lifecycle. Given the interest from academia and the

¹⁵ For instance, Decision Intelligence can support Penetration Testing and Personal Data Protection listed from Step 3 (among others – 28 with practical examples, 7 with marginal/niche applications); SIEM with Application Security, Authentication and AC and so on (direct application in 18, marginal link with 9).

¹⁶ Cryptography, TTPs, data storage (in the context of CS), centralized privacy experience are the remaining missing ones.



potential impact on the security posture of organizations, we will also consider the following for Step 7 grouping and prioritisation:

- Advanced authentication procedures (MFA, conditional AC, behavioural, passwordless);
- Cloud computing, mobile application security, API management and SDKs;
- Cyber Threat Intelligence and cyber deception;
- Security Orchestration Automation and Response (SOAR).

In addition, it is worth also including the security training and awareness and malware threats due to their interest in the reports analysed in Step 4, together with the extracted set of soft skills (which are interdisciplinary with respect to AI, CS and IoT domains).

It is also interesting to highlight the data from Step 3 with more coverage over the topics/technologies from the CS questionnaire (Step 4). The list of those who cover at least half of the topics/technologies (which therefore carries major benefits if explored in depth) are:

- Cloud applications and infrastructure (in the domain of 41/43 inquired topics/technologies);
- Risk Management and governance (in 38/41);
- Risk assessments (in 36/41);
- Law and compliance (in 35/41);
- System, network and data security (in 34/41);
- Everything as a service (in 33/41);
- Personal data protection (in 34/41);
- DevSecOps (in 32/41);
- IT assessment (in 30/41);
- Application security (in 29/41);
- Intelligence analysis (in 29/41);
- Cyber threat intelligence (in 28/41);
- Cybersecurity Audit (in 28/41);
- Organizational Security (in 28/41);
- Authentication and Access Control (in 27/41);
- Secure software lifecycle (in 26/41);
- Incident management (in 26/41);
- AI-based cybersecurity systems (in 24/41);
- Information security controls assessment (in 24/41);
- Cybersecurity Awareness and Training (in 23/41);
- Information systems (in 23/41);
- Penetration Testing (in 22/41);
- Secure communication protocols (in 22/41).

The following set reports the **AI** topics and technologies which were reported by at least half of the organisations via the questionnaire (Step 5), and are in the context of the data extracted from research papers, statistics, reports, and forecasts (in Step 4):

- Generative AI tools;
- Chatbots;
- Data science;
- Developing standardized frameworks and testbeds for AI;
- Improving the quality and availability of data sets for AI;
- AI Project Planning and Co-Development;
- Machine learning;
- Cyber AI;
- AI and future of education;
- AI and Marketing;
- Human-AI collaboration;
- Secure AI systems;
- Effect of AI on social and occupational well being;
- Ethical issues;
- Artificial Intelligence (AI) in higher education (such as teaching in the AI era);
- Role of AI in software.



Considering that Large Language Models (LLM) empower natural language understanding and enhance chatbots, while Explainable AI ensures transparency and trust in AI systems, and their growing interest in academia, we will also consider them for Step 7 grouping and prioritisation.

Considering the results of Step 4 in the context of AI, all topics/technologies and fields were deemed of interest by at least half of the inquired organisations. The top three are:

- AI for algorithm designing;
- Adoption of new technology;
- AI for product marketing.

Compared with the list of topics and skills from the first-year edition, the current one focuses more on potentially disruptive novel technologies (such as large language models and generative models) and confirms high interest on the basis for an effective exploitation of AI (machine learning & data science, high quality dataset, and standardized AI frameworks). Furthermore, a significant loss of interest on specific tools is compensated by an increased attention to emerging applications (such as education, marketing, robotics) and to social and ethical issues.

The following set reports the **IoT** topics and technologies which were reported by at least half of the organisations via the questionnaire (Step 5), and are in the context of the data extracted from research papers, statistics, reports, and forecasts (in Step 4):

- Smart home (e.g., water leak detector, smart lighting);
- IoT platforms (e.g., Azure IoT);
- Smart transportation (e.g., traffic management, parking management, billboard monitoring);
- smart industry (e.g., product management, energy saving, product tracking);
- Smart cities technologies;
- Digital twins;
- Smart environment applications (e.g., measure level of water and flow, air quality monitoring);
- Sensors for monitoring students' behavior and to support personalized learning;
- Edge analytics;
- Intelligent sensors;
- Cellular IoT (2G - 5G);
- Data ecosystems;
- Data spaces;
- TinyML.

Considering the ethical and social implications¹⁷ of monitoring students' behaviour in classrooms (although to support personalised learning) and the risks of data breach and privacy violations (with possible fines associated with the General Data Protection Regulation - GDPR), we will not consider it in Step 7 grouping and prioritization.

¹⁷ For instance the fairness of automated processing (which, however, could be supported by explainable AI), the interests of stakeholders, or more generally the difficulty of professors and students interacting with each other knowing they are being monitored.



Following is the list of the IoT data from Step 3 with more coverage over the topics/technologies from the IoT questionnaire (Step 4) - at least half of the topics/technologies.

- Distributed System;
- Machine learning and artificial intelligence (e.g., to obtain advanced insights or for decision-making);
- Real-time monitoring;
- Authentication and Access Control and more general cybersecurity measures;
- Application layer protocols (such as DDS, COAP, AMQP, MQTT, MQTT-SN, XMPP, COAP);
- Routing protocols (e.g., 6LOWPAN);
- Physical/device layer protocols (LTE-A, EPCglobal, Z-Wave);
- IoT platforms (e.g., Azure or AWS);
- Service-oriented applications (SOA);
- The use of IoT in energy, industry and healthcare scenarios;
- Cyber-physical systems;
- Big data and analytics;
- Cloud, edge, and fog computing;
- Smart cars and Smart cities, smart homes, and smart grids applications.

Compared with the list of topics and skills from the first-year edition, the current one once again highlights the importance of IoT protocols and confirms the interest in IoT security, but loses specificity with respect to big data tools and do not directly mention industrial automation, sensors and actuators.

Step 7) Use the set of skills highlighted by consortium Universities to prioritize the set of topics that will be considered when creating/updating the MERIT programme. In the following, we merge Step 6 topics and skills with the envisaged set of skills extracted as part of Step 2 and indicate for each of the three domains those that should be prioritised in MERIT master programs and related activities.

Results

In the **Cybersecurity** domain:

Table 3: Prioritised list of Cybersecurity topics, technologies and application areas for MERIT courses and related activities.

	Cybersecurity Topic or Technology to be provided; Skill or Expertise (in specific application areas) to be developed	To prioritize
Fundamental knowledge	Monitoring of large-scale and interconnected systems: This involves overseeing complex systems, networks, and applications to detect anomalies, performance issues, and security threats. Understanding the principles of monitoring and how to analyze system behavior is crucial for cybersecurity professionals. (Ref. to CS-Q1 in the following Scopus search and in Appendix A).	X*
	Threat Modeling: A structured approach to identifying and assessing potential threats to a system or application. It helps in designing secure systems by anticipating and addressing vulnerabilities early in the development process. (Ref. to CS-Q2).	X
	Zero Trust principles (Zero Trust Network Access - ZTNA): A security model that assumes no inherent trust within a network, requiring verification for every access attempt. Understanding Zero Trust architecture is foundational for securing modern networks. (Ref. to CS-Q3).	X
	Risk Management and governance: Managing risks, compliance, and organizational policies. Cybersecurity professionals need to understand risk assessment, mitigation strategies, and legal and ethical considerations. (Ref. to CS-Q4).	X



Applied Knowledge	Machine learning with context-awareness: Leveraging machine learning techniques to adapt and make decisions based on contextual information. This skill is valuable for anomaly detection, threat prediction, and adaptive security measures. (Ref. to CS-Q5).	X*
	DevSecOps: Integrating security practices into the DevOps process, ensuring security is part of the software development lifecycle. Practical experience in implementing security controls within agile development environments is essential. (Ref. to CS-Q6).	
	Security Orchestration Automation and Response (SOAR): Coordinating security processes through automation and orchestration. This involves leveraging cyber threat intelligence and automated workflows to respond effectively to incidents. (Ref. to CS-Q7).	X*
	Cloud computing, mobile application security, API management, and SDKs: Ensuring security across cloud services (more generally XaaS), mobile apps, APIs, and software development kits. Practical knowledge of securing cloud environments and mobile applications is crucial. (Ref. to CS-Q8).	X
	Incident management: Handling security incidents promptly and effectively. Practical experience in incident response, including containment, eradication, and recovery, is essential. (Ref. to CS-Q9).	
	AI-based cybersecurity systems: Utilizing artificial intelligence for threat detection, prevention, and response. Practical skills in implementing AI-driven security solutions are valuable. (Ref. to CS-Q10).	X
	Penetration Testing: Ethical hacking to identify vulnerabilities in systems. Practical experience in conducting security assessments and vulnerability testing is essential. (Ref. to CS-Q11).	X
	Secure communication protocols: Ensuring secure data transmission over networks. Practical knowledge of encryption, secure channels, and cryptographic protocols is necessary. (Ref. to CS-Q12).	
	Advanced Authentication Procedures: Implementing secure authentication methods, including multi-factor authentication (MFA), conditional access (AC), and behavioral authentication. Practical experience in configuring and managing authentication mechanisms is important. (Ref. to CS-Q13).	X*
	Personal data protection: Safeguarding sensitive personal information from unauthorized access or disclosure. Practical knowledge of data privacy laws, encryption, and access controls is critical. (Ref. to CS-Q14).	X

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 growing interest in the use of artificial intelligence in cybersecurity (CS-Q10, 204 slope¹⁸ value); followed by a persistent and growing interest in the security of cloud computing, mobile application security, and API management (CS-Q8, 83); then zero trust (CS-Q3, 78); threat modelling (CS-Q2, 49); penetration testing (CS-Q11, 34); personal data protection (CS-Q14, 12); and risk management and governance (CS-Q4, 11). Nonetheless, considering our research experience with some of the reported topics, technologies and areas, and the huge difference in interest of the industries reported in the step 4 questionnaire, we decided to prioritize also advanced authentication procedures; Security Orchestration Automation and Response (SOAR); Monitoring of large-scale and interconnected systems and machine learning with context awareness. Those have been indicated with “X*” in Table 3 above.

¹⁸ 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>.



MERIT Deliverable



Co-funded by the European Union

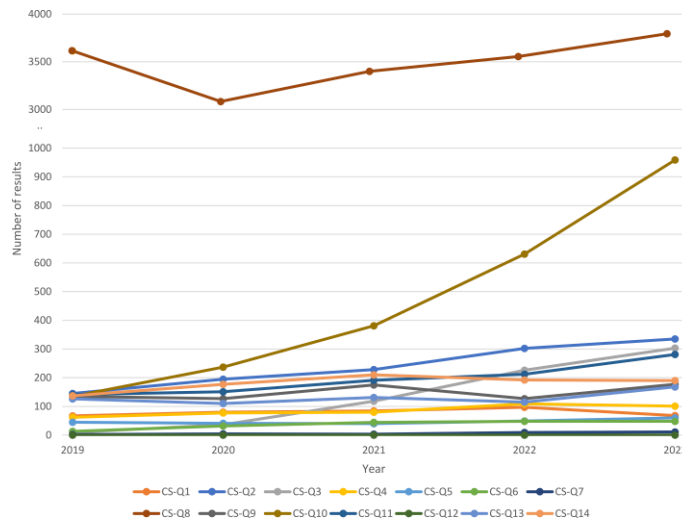


Figure 3: Academic interest in the reported CS topics, technologies and application areas in the past five years using Scopus and specific queries and parameters (ref. to Appendix A).

In the **Artificial Intelligence** domain:

Table 4: Prioritised list of Artificial Intelligence topics, technologies and application areas for MERIT courses and related activities.

	Artificial Intelligence Topic or Technology to be provided; Skill or Expertise (in specific application areas) to be developed	To prioritize
Fundamental knowledge	Machine learning, Ethical issues, Knowledge representation and reasoning, planning, search, and optimization, Large Language Models (LLM), Explainable AI. (Ref. to AI-Q1 in the following Scopus search and in Appendix A).	X
	Generative AI tools, Cyber AI, Secure AI systems, Role of AI in software, AI for algorithm designing, Critical thinking and analysis, Complex problem solving, Active learning, Machine learning technologies. (Ref. to AI-Q2).	
	Improving the quality and availability of data sets for AI. (Ref. to AI-Q3).	X
	Data science, Big data, Data processing and management. (Ref. to AI-Q4).	
	AI tools and technology for reasoning, AI for technology design and programming. (Ref. to AI-Q5).	X
Applied Knowledge	Developing standardized frameworks and testbeds for AI, AI Project Planning and Co-Development, problem-solving and ideation. (Ref. to AI-Q6).	
	AI Applications: Chatbots, AI and Marketing, Artificial Intelligence (AI) in higher education, AI for product marketing, Manufacturing, AI in space industry (more generally spatial data processing), Analytical thinking and innovation. (Ref. to AI-Q7).	X
	AI Applications: AI and future of education, Human-AI collaboration, Effect of AI on social and occupational well-being, Adoption of new technology, Autonomous driving, AI for business management, Digital marketing AI with cloud technologies. (Ref. to AI-Q8).	
	AI Adoption: AI adoption index. (Ref. to AI-Q9).	

The Scopus investigation (detailed in Figure 4) reveals a growing interest in literature with the first two groups of topics, technologies and skills (AI-Q1 slope value 3919, AI-Q2 value 3878); however, we believe the first applied knowledge (AI-Q7 value 734) to be prioritized given the wide diffusion of chatbots (and their ability to handle large volumes of customers), the benefits of AI in marketing (to derive customer insights, automating critical marketing decision and delivering personalized experi-



ences at scale), and more generally analyze vast amount of data at unprecedented speed or automate repetitive tasks. Similar considerations apply with respect to AI-Q8 (value 1042) application areas.

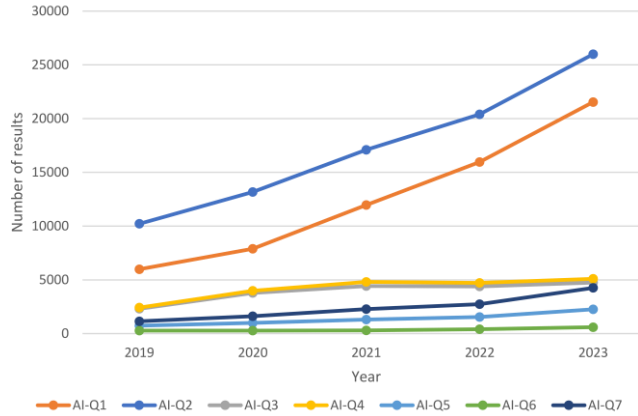


Figure 4: Academic interest in the reported AI topics, technologies and application areas in the past five years using Scopus and specific queries and parameters (ref. to Appendix A).

For courses and activities on the **Internet of Things** domain:

Table 5: Prioritised list of Internet of Things topics, technologies and application areas for MERIT courses and activities.

	Internet of Things Topic or Technology to be provided; Skill or Expertise (in specific application areas) to be developed	To prioritize
Fundamental knowledge	IoT Platforms and Services: Understanding of IoT platforms such as Azure or AWS IoT, service-oriented applications (SOA), data ecosystems, data spaces, edge analytics, and cloud, edge, and fog computing. (Ref. to IoT-Q1 in the following Scopus search and in Appendix A).	X
	IoT Communication Protocols: Knowledge of application layer protocols (DDS, COAP, AMQP, MQTT, MQTT-SN, XMPP), routing protocols (6LOW-PAN), and physical/device layer protocols (LTE-A, EPCglobal, Z-Wave). (Ref. to IoT-Q2).	
	Advanced Technologies and Concepts: Understanding of machine learning and artificial intelligence, TinyML, cyber-physical systems, big data and analytics, and distributed systems. (Ref. to IoT-Q3).	X
	Authentication and Access Control: Basic understanding of cybersecurity measures. (Ref. to IoT-Q4).	
Applied Knowledge	Smart Environments and Applications: Practical knowledge of smart home, smart transportation, smart industry, smart cities technologies, smart environment applications, digital twins, intelligent sensors, real-time monitoring. (Ref. to IoT-Q5).	X
	Use Cases: Practical understanding of the use of IoT in energy, industry, and healthcare scenarios, cellular IoT (2G to 5G), smart cars and smart cities, smart homes, and smart grids applications. (Ref. to IoT-Q6).	X

We fully support the Scopus investigation (detailed in Figure 5) on the set of foundational and applied knowledge skillset: IoT-Q3 with a slope of 1124, IoT-Q5 with 1014, IoT-Q6 with 889, IoT-Q1 with 458 and IoT-Q4 with 191.



MERIT Deliverable



Co-funded by
the European Union

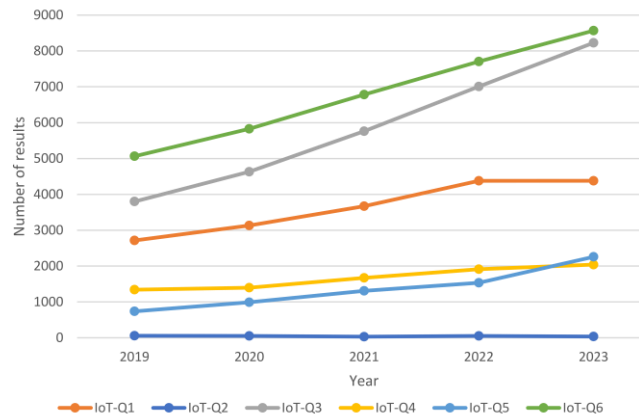


Figure 5: Academic interest in the reported IoT topics, technologies and application areas in the past five years using Scopus and specific queries and parameters (ref. to Appendix A).

Considering the soft skills, MERIT HEIs 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 emphasized.
- 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 Behavior: Adherence to professional and ethical behavior principles is expected.
- Understanding Legal and Social Aspects: They should understand the legal and social aspects of system management.
- Continuous Learning: All universities emphasize the importance of continuous learning.
- Ethical Standards: Adherence to ethical standards is expected.

Nonetheless, the remaining envisaged set of soft skills constitute an important wealth of experience that could support them both at work and in life:

- Innovation: They should be able to create innovative solutions.
- Justification: They should be able to justify their solutions.
- Security Analysis: They should be able to analyse security weaknesses.
- Proposing Solutions: They should have the ability to propose innovative and sustainable solutions.

Compared with the list of topics and skills from the first-year edition, the current one is more balanced: more space is given to artificial intelligence (from 1 to 11 topics, technologies, and application areas) and IoT (from 1 to 5); additional space also to soft-skills (from 2-3 to 11). The list also highlights the influence of AI in cybersecurity and IoT (e.g., leveraging the potential of machine learning). Cloud



computing, Zero Trust, IoT security, big data and analytics, Personal data protection¹⁹, DevSecOps²⁰, all remain important also in the second edition.

To verify the current integration of Table 3 (for CS), Table 4 (AI) and Table 5 (IoT) topics, technologies, and applications areas in the MERIT master programs, we adopted the strategy described in the MERIT Milestone MS6: we initially extracted a set of representative keywords from the aforementioned tables; then extracted a set of representative keywords from MERIT courses (as defined in Universities syllabi); finally, verified the correspondence using the Sentence Transformer model and the topic similarity (cosine) estimation²¹ - we used a threshold of 0.5. The comparison also used a Google AppScript script to aid the evaluation.

Upon 29 entries (corresponding to Table 4, Table 5 and Table 6 rows) 25 were covered by at least one of the courses planned by MERIT Universities, and 2 by at least one course in each University (those associated with IoT-Q3 and IoT-Q6 queries). 15 entries among the 25 covered ones are those we recommended to be prioritised. This result demonstrates that, even if the syllabi were defined before performing the analysis described in this document, they are already moderately updated. In addition, now MERIT consortium Universities will have the possibility to better plan the exchange of resources (for instance, leveraging other MERIT University courses to cover specific topics) or integrate the topics, technologies, and areas before the start of master programs to be on the edge of what was found from literature and from industry needs.

To understand how the results of the second edition of the methodology align with the European skills and labour market, we assessed as in D3.1 their adherence to the European Skills, Competences, Qualifications and Occupations (ESCO) [24] classification, and to the European e-Competence Framework (e-CF) [25].

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 29 keywords from Step 7 and the *Full Text Search* API. We obtained 3770 results (2297 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 655 results (247 related to the AI domain, 259 and 149 to CS and IoT ones – respectively). To assess them, we used the script²² developed for the first application of the methodology to:

- Query the ESCO database for each of the 655 results using the *Full Text Search* API.
- Fetch related "essential for" occupations (if listed) and the ESCO identification code (if available). If not available, fetch the parent in the ESCO classification hierarchy and its type (Knowledge or Skill).
 - For Transversal Knowledge items, duplicate parents, or results classified as "obsolete" by ESCO, manually query the online database to identify the parent or alternative labels.
- Classify the results into the AI, CS, and IoT.

The mapping²³ resulted in 662 low-level items:

- 332 unique skills: 154 associated with the CS domain, 148 with AI, and 72 with IoT.
- 237 unique knowledge items: 112 in the CS domain, 104 in AI, and 44 in IoT.

To gain a broader perspective on the skills and knowledge items, we considered parent items in the ESCO classification hierarchy, which returned the following:

¹⁹ If we consider including the *Cybersecurity-related laws, regulations, or legislations; and their requirements* from the first edition, as provided in the description in the CS table.

²⁰ If we consider including the *Security by-design and Secure-software development lifecycle (SSDLC)* from the first edition.

²¹ Ref. to <https://huggingface.co/sentence-transformers> and MERIT MS6 report for additional information.

²² Available at https://digitalmerit.eu/wp-content/uploads/2024/07/MERIT_ESCO_code.zip.

²³ Available at <https://digitalmerit.eu/wp-content/uploads/2024/07/ESCO-Mapping.zip>. Appendix C provides a synthesis of the algorithm.



- 97 unique skills: 53 in the CS domain, 59 in AI, and 44 in IoT.
- 45 unique knowledge items: 22 in the CS domain, 31 in AI and 22 in IoT.

According to the ESCO classification, the knowledge of topics, technologies, and skills identified in Step 7 would enable MERIT students to access 1539 possible occupations (881 related to CS, 950 to AI, and 391 to IoT).

Comparing those results with the first application of the methodology, there is an increment on the number of skills and knowledge items covered by the list in Step 7 (42% and 49%, respectively). We believe this to be even more valuable considering the evaluation and filtering, which removed 3115 results as out of context (3770 to the 655 results used by the script), many more than those removed in the first application (3097 to 1271).

Regarding the e-CF framework, we manually mapped which roles from the framework could be associated with Step 7 skills, topics, and technologies. We initially verified the skill level (among the five available skill groups) to which we could map the Step 7 results.

- Monitoring of large-scale and interconnected systems: A.1 (L4, L5), A.5 (L4), C.3 (L3), C.5 (L3), E.3 (L2 to L4).
- Threat Modeling: A.1 (L4, L5), D.1 (L4, L5), E.8 (L2 to L4).
- Zero Trust; Zero Trust Network Access (ZTNA): D.1 (L4, L5), E.8 (L2 to L4).
- Risk Management and governance: A.1 (L4, L5), D.1 (L4, L5), E.3 (L2 to L4).
- Machine learning with context-awareness: A.7 (L4, L5), A.9 (L4, L5), D.7 (L3 to L5).
- DevSecOps: B.1 (L3), B.3 (L3), B.4 (L3), E.2 (L3 to L5).
- Security Orchestration Automation and Response (SOAR): C.2 (L3, L4), E.8 (L2 to L4).
- Cloud computing security; XaaS; mobile application security; API management; Software Development Kits (SDKs): A.1 (L4, L5), A.5 (L4), C.3 (L3), C.5 (L3), E.8 (L2 to L4).
- Incident management: C.2 (L3, L4), E.8 (L2 to L4).
- AI-based cybersecurity systems: A.7 (L4, L5), A.9 (L4, L5), D.7 (L3 to L5).
- Penetration Testing; ethical hacking: B.1 (L3), B.3 (L3), E.8 (L2 to L4).
- Secure communication protocols: D.1 (L4, L5), E.8 (L2 to L4).
- Advanced Authentication Procedures: D.1 (L4, L5), E.8 (L2 to L4).
- Personal data protection: D.1 (L4, L5), E.8 (L2 to L4).
- Artificial intelligence; Machine learning; Ethical issues, Knowledge representation and reasoning, planning; search and optimization; Large Language Models (LLM); Explainable Artificial Intelligence: A.7 (L4, L5), A.9 (L4, L5), D.7 (L3 to L5).
- Generative Artificial Intelligence tools; Cyber Artificial Intelligence; Secure Artificial Intelligence systems; Role of Artificial Intelligence in software; Artificial Intelligence for algorithm designing; Critical thinking and analysis; Complex problem solving; Active learning; Machine learning technologies: A.7 (L4, L5), A.9 (L4, L5), D.7 (L3 to L5).
- Improving the quality and availability of data sets for Artificial Intelligence; data quality; big data processing: A.7 (L4, L5), D.7 (L3 to L5).
- Data science; Big data; Data processing and management: A.7 (L4, L5), D.7 (L3 to L5).
- Artificial Intelligence tools and technology for reasoning; Artificial Intelligence for technology design and programming: A.7 (L4, L5), A.9 (L4, L5), D.7 (L3 to L5).
- Developing standardized frameworks and testbeds for Artificial Intelligence; Artificial Intelligence Project Planning and Co-Development; problem-solving and ideation: A.7 (L4, L5), A.9 (L4, L5), D.7 (L3 to L5).
- Artificial Intelligence Applications; Chatbots; Artificial Intelligence and Marketing; Artificial Intelligence in higher education; Artificial Intelligence for product marketing; Artificial Intelligence for Manufacturing; Artificial Intelligence in space industry (more generally spatial data processing); Analytical thinking and innovation: A.7 (L4, L5), A.9 (L4, L5), D.7 (L3 to L5).



- Artificial Intelligence Applications; Artificial Intelligence and future of education; Human-Artificial Intelligence collaboration; Effect of Artificial Intelligence on social and occupational well-being; Adoption of new technology; Autonomous driving; Artificial Intelligence for business management; Digital marketing; Artificial Intelligence with cloud technologies: A.7 (L4, L5), A.9 (L4, L5), D.7 (L3 to L5).
- Artificial Intelligence adoption index: A.7 (L4, L5), A.9 (L4, L5), D.7 (L3 to L5).
- IoT Platforms and Services; understanding of IoT platforms such as Azure or AWS IoT, service-oriented applications (SOA); data ecosystems; data spaces; edge analytics; cloud, edge, and fog computing: A.1 (L4, L5), A.5 (L4), C.3 (L3), C.5 (L3), D.7 (L3 to L5).
- IoT Communication Protocols; knowledge of application layer protocols (such as DDS, COAP, AMQP, MQTT, MQTT-SN, XMPP), routing protocols (such as 6LOWPAN), and physical/device layer protocols (such as LTE-A, EPCglobal, Z-Wave): A.1 (L4, L5), A.5 (L4), C.3 (L3), C.5 (L3), D.7 (L3 to L5).
- Advanced Technologies and Concepts; understanding of machine learning and artificial intelligence; TinyML; cyber-physical systems; big data and analytics; distributed systems: A.7 (L4, L5), A.9 (L4, L5), D.7 (L3 to L5).
- Authentication and Access Control; cybersecurity measures: D.1 (L4, L5), E.8 (L2 to L4).
- Smart Environments and Applications; smart home; smart transportation; smart industry; smart cities technologies; smart environment applications; digital twins; intelligent sensors; real-time monitoring: A.1 (L4, L5), A.5 (L4), C.3 (L3), C.5 (L3), D.7 (L3 to L5).
- Use of IoT in energy, industry, and healthcare scenarios; cellular IoT (2G to 5G); smart cars and smart cities applications; smart homes applications; smart grids applications: A.1 (L4, L5), A.5 (L4), C.3 (L3), C.5 (L3), D.7 (L3 to L5).

Those allow the partial coverage²⁴ of the following e-CF roles:

- account manager.
- business analyst.
- business information manager.
- chief information officer.
- data scientist.
- data specialist.
- database administrator.
- developer.
- devops expert.
- digital media specialist.
- digital transformation leader.
- enterprise architect.
- ict operations manager.
- information security manager.
- information security specialist.
- network specialist.
- product owner.
- project manager.
- quality assurance manager.
- scrum master.
- service support.
- solution designer.
- systems administrator.
- systems analyst.
- systems architect.
- technical specialist.
- test specialist.

Comparing the results with the first application of the methodology, we were able to find a mapping for all Step 7 results. Considering e-CF skill levels, this edition covers also A7, A9, B3 and B4; C2, C3 and C5, and E2. It does not cover instead B2, B6, C4, D3 and D6 (as the list in Step 7 of D3.1).

²⁴ For instance, to cover all competences of the *database administrator* role, Step 7 results must have included also a map to B.2 (Component Integration) and D.10 (Information and Knowledge Management).



3 Roles of AI-CS and AI-IoT

In this section, we elaborate on the role of Artificial Intelligence in the domains of Cybersecurity and IoT. We classify AI in two main categories: classical machine learning techniques (such as supervised learning, unsupervised learning, and reinforcement learning) and generative AI techniques (for instance, Large Language Models).

- **Classical AI (e.g. machine learning) in Cyber Security**

Machine learning techniques applied to Cybersecurity allow for improving the accuracy of threat detection (both active and proactive), accelerating incident investigations, and improving the automation in response.

Common applications are:

1. Advanced threat detection (network, endpoint, and identity)
 - a. Improve anti-phishing mechanisms and cybersecurity awareness with NLP to counter social engineering attacks, such as those that adopt AI-generated voice fakes and deep fakes.
 - b. Provide behavioural analytics.
2. Improving authentication
 - a. Dynamically evaluate the risk of authenticated users (e.g., as employed by Microsoft and IBM²⁵).
 - b. Support biometric authentication.
3. Vulnerability assessment and threat response
 - a. Analyse real-time data and prioritize vulnerabilities based on the risk score/level.

- **Roles of Classical AI (Machine Learning) to mitigate Cybersecurity related issues.**

The intersection between AI and CS expertise is particularly evident in the following activities:

1. Threat detection:
 - a. AI models can automatically recognize patterns in network traffic, emails, and other data that may indicate a security threat.
 - b. They can also be used to identify malware and other malicious activities automatically.
2. Intrusion detection and prevention:
 - a. It's helpful for detection intrusions in real time and block or mitigate them automatically.
 - b. This helps prevent security breaches and minimize the damage they cause.
3. Anomaly detection:
 - a. It's helpful to identify anomalies in data that might indicate a security threat, such as unusual user behaviour or a spike in network traffic.
4. Vulnerability management:
 - a. AI helpful in the process of identifying and fixing vulnerabilities in software and systems, reducing the risk of exploitation by malicious actors.
5. Fraud detection:
 - a. To identify fraudulent activities, such as phishing attacks, credit card fraud, and other types of financial scams.

²⁵ As reported by Microsoft in <https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa> and IBM in https://www.ibm.com/docs/en/SS42VS_SHR/com.ibm.UBAapp.doc/c_Qapps_UBA_intro.html.



- **Generative AI (large language models) Roles to mitigate Cybersecurity related issues.**

Generative AI specifically Large Language Models (LLM), including those leveraging AI, playing crucial roles in cyber security landscape. Below are some specific skills, working positions and applications where these models are commonly utilized.

- **Common skills needed for LLM experts:**

- Programming,
- Natural Language Processing.
- Mathematics & Statistics, Machine Learning and Deep Learning, Reinforcement Learning and Reinforcement Learning with Human Feedback (RLHF).
- Model Architectures, Model Fine tuning.
- Problem solving, Domain Knowledge, Ethics, Bias Awareness, Continuous Learning and Critical Thinking and Problem-Solving.

By developing proficiency in these skills, individuals can effectively work with large language models and contribute to advancements in the field of natural language processing and artificial intelligence.

1. **Threat Intelligence Analysts:**

- a. Cybersecurity, threat intelligence, and natural language processing (NLP), Here are the key skills required.
- b. Cybersecurity Fundamentals, Scripting, Data Analysis and Visualization.
- c. Cyber Threat Landscape Knowledge.
- d. Open-Source Intelligence (OSINT), Communication and Collaboration, Ethical and Legal Awareness.

2. **Security Operations Centre (SOC) Analysts:**

- a. Cybersecurity, threat intelligence, and natural language processing (NLP), Here are the key skills required.
- b. Cybersecurity Fundamentals, Knowledge of SOC Operations, Model Interpretability and Explainability.
- c. Threat Hunting and Detection, Incident Response and Mitigation, Compliance and Regulatory Knowledge and Continuous Learning and Adaptability.
- d. By acquiring these skills, you can effectively leverage LLMs to enhance SOC operations, improve threat detection and response capabilities, and strengthen overall cybersecurity posture.
- e. Language models assist SOC analysts in processing and understanding security alerts, parsing logs, and correlating information to detect and respond to potential cyber threats.

3. **Incident Responders:**

- a. Cybersecurity, threat intelligence, and natural language processing (NLP), Here are the key skills required.
- b. Cybersecurity Fundamentals, Data Analysis and Visualization.
- c. Cyber Threat Landscape Knowledge, Open-Source Intelligence (OSINT), Critical Thinking and Problem-Solving, Communication and Collaboration, Ethical and Legal Awareness.

4. **Phishing Detection Specialists:**

- a. Cybersecurity, threat intelligence, and natural language processing (NLP), Here are the key skills required.
- b. Cybersecurity Fundamentals, Cyber Threat Landscape Knowledge, Critical Thinking and Problem-Solving, Phishing Awareness and Domain Knowledge.

5. **Malware Analysts:**

- a. Cybersecurity, threat intelligence, and natural language processing (NLP), Here are the key skills required.
- b. Cybersecurity Fundamentals, Open-Source Intelligence (OSINT), Critical Thinking and Problem-Solving.
- c. Communication and Collaboration, Ethical and Legal Awareness, Tool Familiarity and Malware Analysis Techniques.

6. **Security Consultants:**



- a. Cybersecurity, threat intelligence, and natural language processing (NLP), Here are the key skills required.
 - b. Cybersecurity Fundamentals, Open-Source Intelligence (OSINT), Critical Thinking and Problem-Solving, Communication and Collaboration, Ethical and Legal Awareness, Incident Response and Forensics, Compliance and Regulatory Knowledge, Security Testing and Evaluation and Privacy and Confidentiality
- 7. Automated Threat Hunting:**
- a. Cybersecurity, threat intelligence, and natural language processing (NLP), Here are the key skills required.
 - b. Cybersecurity Fundamentals, Ethical and Legal Awareness.
 - c. Big Data Technologies, Ethical Hacking and Penetration Testing, and Security Tools and Frameworks.
 - d. AI-powered language models can automate the process of searching for potential threats in large datasets, logs, and network traffic, enhancing the efficiency of threat hunting activities.
- 8. Policy and Compliance Analysts:**
- a. Cybersecurity, threat intelligence, and natural language processing (NLP), Here are the key skills required.
 - b. Cybersecurity Fundamentals.
 - c. Critical Thinking and Problem-Solving, Communication and Collaboration, Ethical and Legal Awareness, Policy Analysis.
 - d. Regulatory Compliance, Data Privacy and Security, Risk Management, Ethics and Responsible AI, Legal Research and Interpretation and Project Management.
- By developing and leveraging these skills, Policy and Compliance Analysts can effectively navigate the intersection of AI technologies, such as large language models, and regulatory frameworks to ensure responsible and compliant use in various industries and domains. These positions highlight the diverse applications of large language models in Cybersecurity, contributing to more effective and efficient threat detection, response, and overall security posture.

In conclusion, we have explored the potential roles of AI within the realms of machine learning and the emerging era of generative artificial intelligence. Essentially, the rise of large language models is causing disruptions across various fields. Figure 6, which we also provided in D3.1, shows an overview of the artificial intelligence landscape within the data sphere in perspective of machine learning. Initially, we outline application domains such as manufacturing, education, and healthcare, where AI stands to make a substantial impact. Additionally, we highlight the fundamental components necessary to facilitate real-time deployment of AI within a particular domain. Each role entails specific job prerequisites, and we further categorize them into standard and domain-specific skills, along with prospective proficiencies required to tackle intricate challenges in the future.

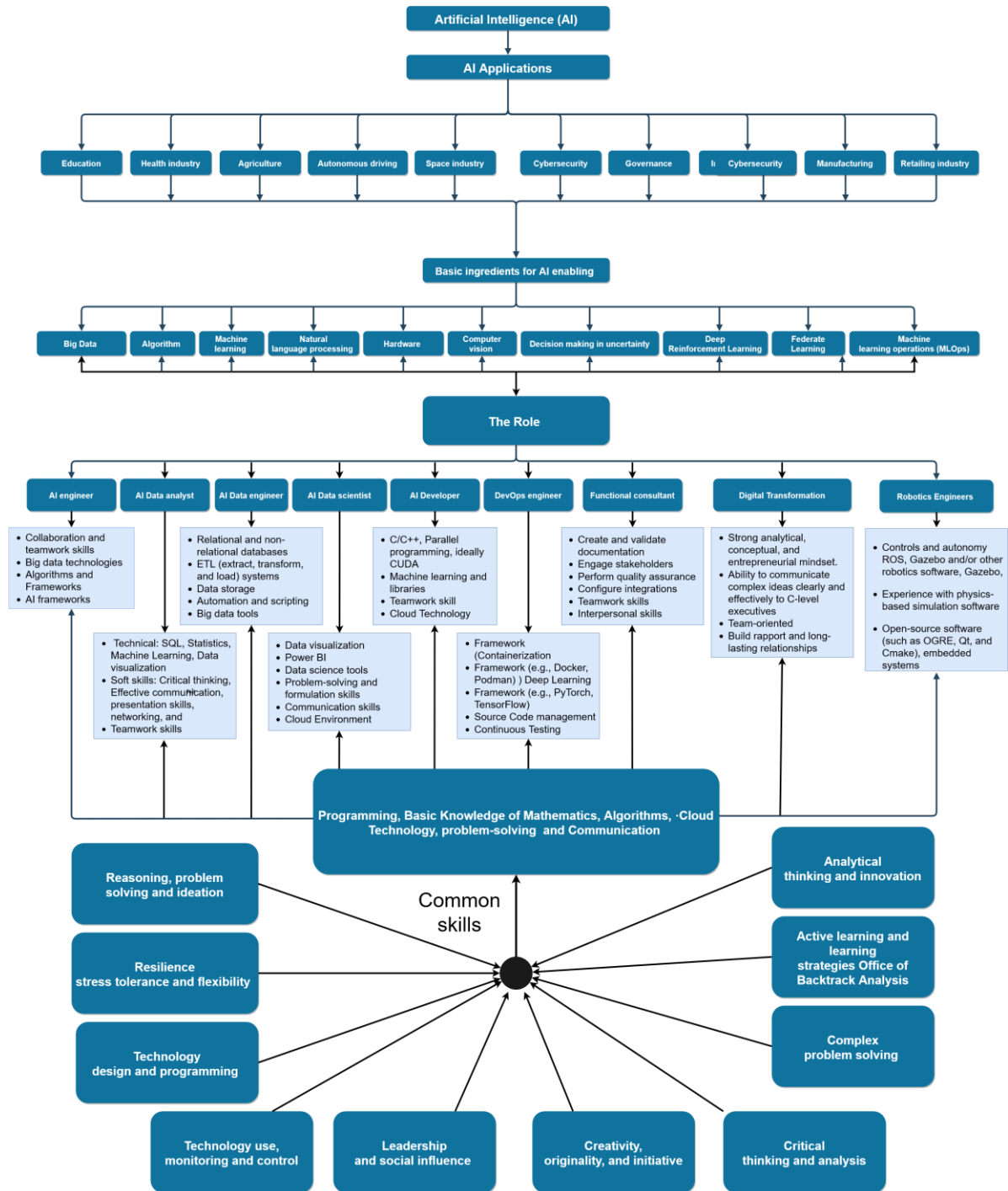


Figure 6: Framework for AI roles, common skills, and specific skills in age of industrial data space.



4 Conclusions

This document presents the methodology to identify and prioritize the most relevant topics and skills for the consortium Universities (to upgrade and deliver the master programme), and for the MERIT communication and dissemination activities. The second application of the methodology provides seven results in line with the methodology steps:

1. The current MERIT Partners' areas of expertise, that allowed focusing their effort in identifying the current and forecasted topics and skills for D3.3; and can also be used when preparing the material for the master programme (WP5), and for both the educators upskilling and their mobility between Universities (WP6).
2. The envisaged set of skills by MERIT HEIs for their future graduates, updated extracting those from MERIT study programs.
3. A new carefully crafted set of data sources and keywords identified by MERIT Partners to investigate current and forecasted topics and skills in AI, CS and IoT.
4. A set of 83 topics, technologies and innovative scenarios identified from research, statistics, reports and forecasts that are crucial to update 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.
5. A set of 50 topics, technologies and application scenarios adopted currently or up to the next two years by 30 SMEs inquired via questionnaires in MERIT partners' regions, which highlight the current industry needs; and are essential to make the study programs operational.
6. A carefully defined mapping of topics, technologies and application scenarios with the industry needs to highlight those with interest from both industry and academia: 25 possible CS, AI and IoT topics, 25 technologies and 30 application scenarios.
7. A prioritized list of 45 topics and technologies (also considering the description from the tables) and 16 application scenarios that can be used update the MERIT study program and related activities.
 - a. Evaluating the list in the context of the ESCO [24] framework, we found that the acquisition of these knowledge, technologies and skills is linked with 332 unique skills and 237 knowledge items, spans multiple application scenarios (from finance to healthcare) and provides access to 1539 job positions. The combination of automated querying and manual investigation ensured comprehensive coverage and accuracy. Future work could focus on improving even more the algorithm to handle ambiguous cases better.
 - b. Considering the e-CF framework, we mapped Step 7 results to 15 e-CF competences and leveraging competences to 27 e-CF roles.

The following general insights can be derived from the second iteration of the methodology:

- MERIT HEIs focus their master programs on different specific domains, from AI (without CS among core courses) to manufacturing and economics, but they all agree on applying foundational knowledge in practice and providing a set of soft skills that help future graduates in life. In addition, the possible sharing of AI, CS and IoT expertise is fostered by the sharing of (elective) courses, materials and lecturers in line with the MERIT consortium agreements.
- The topics and technologies, as well as the application scenarios, highlighted in the questionnaires, seem to deviate from those obtained from the analysis in the literature: this demonstrates a gap between research and industry which on one hand can highlight delays in the adoption of cutting-edge technologies; and on the other, the need to obtain a larger survey sample.
- As already reported in the first application of the methodology, a standardised approach to identify the professional roles is essential to determine current and future skill gaps: agencies like ENISA or



MERIT Deliverable



Co-funded by
the European Union



research projects funded by the European Commission play a leading role in identifying and defining required skills. One of the examples mentioned in the document is the European Cybersecurity Skills Framework (ECSF) via the EU REWIRE project.

- All three areas share, from both the research and industry perspective, the need for both technical and soft skills. This year, we have chosen to give greater emphasis to these skills in line with MERIT HEIs expectations for their graduates.
- Acquiring expertise common to the three areas (AI, CS and IoT) opens to highly specialized professional figures, with wider career prospects: for instance, using AI in the context of Threat Intelligence (in a CS working role) or securing AI algorithms (in an “AI”-oriented role) can both share a substantial portion of expertise.
- The document offers a comprehensive understanding of the domains encompassing AI, CS, and IoT, focusing on current and future technological trends, roles, and serving as a cornerstone in the field of future studies programs.
- It provides mapping of fields (e.g. manufacturing and health), technologies and future roles, which could also be leveraged by recruiters for hiring procedures.

As reported in D3.1, projects with the goal of advancing digital skills like MERIT share the task and responsibility to highlight and leverage the synergies of multiple domains (AI, CS and IoT); and have the opportunity to support the current and future skill gaps by training and upskilling on the most relevant and needed topics.



References

- [1] D. Zowghi and C. Coulin, "Requirements Elicitation: A Survey of Techniques, Approaches, and Tools," in *Engineering and Managing Software Requirements*, 2005.
- [2] M. Gusenbauer and N. Haddaway, "Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources," *Research synthesis methods*, 2020.
- [3] REWIRE, "R5.2.1 Annual Cybersecurity Skills Trends Report," 2023.
- [4] REWIRE, "R5.2.1 Second Annual Cybersecurity Skills Trends Report," 2023.
- [5] ENISA, "European Cybersecurity Skills Framework Role Profiles," 2022.
- [6] ENISA, "Foresight Cybersecurity Threats for 2030," 2023.
- [7] CLUSIT, "Rapporto Clusit 2023," 2023.
- [8] D. Bendler and M. Felderer, "Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model," *ACM Trans. Comput. Educ.* 23, 2023.
- [9] J. Rajamäki, P. Rathod and K. Kioskli, "Demand Analysis of the Cybersecurity Knowledge Areas and Skills for Nurses: Preliminary Findings," in *22nd European Conference on Cyber Warfare and Security*, 2023.
- [10] Splunk Inc., "The CISO Report," 2023.
- [11] L. B. Furstenu, Y. P. R. Rodrigues, M. K. Sott, P. Leivas, M. S. Dohan, J. R. López-Robles, M. J. Cobo, N. L. Bragazzi and K.-K. R. Choo, "Internet of things: Conceptual network structure, main challenges and future directions," in *Digital Communications and Networks*, 2023.
- [12] A. Sehnaz, C. c. Zaihisma and A. Nor'Ashikin, "A Systematic Review of Internet of Things Adoption in Organizations: Taxonomy, Benefits, Challenges and Critical Factors," in *Applied Sciences*, 2022.
- [13] S.-N. Abolghasem, "Internet of Thing (IoT) review of review: Bibliometric overview since its foundation," in *Future Generation Computer Systems*, 2023.
- [14] S. Bankins, A. C. Ocampo, M. Marrone, S. L. D. Restubog and S. E. Woo, "A multilevel review of artificial intelligence in organizations: Implications for organizational behavior research and practice," *Journal of Organizational Behavior*, 2023.
- [15] M. Weber, M. Engert, N. Schaffer and J. W. a. H. Krcmar, "Organizational Capabilities for AI Implementation—Coping with Inscrutability and Data Dependency in AI," in *Information Systems Frontiers*, 2022.
- [16] E. Anton, A. Behne and F. Teuteberg, "The Humans Behind Artificial Intelligence—An Operationalisation of AI Competencies," in *Twenty-Eighth European Conference on Information Systems (ECIS2020)*, 2020.
- [17] P. Mikalef, N. Islam, V. Parida, H. Singh and N. Altwaijry, "Artificial intelligence (AI) competencies for organizational performance: A B2B marketing capabilities perspective," *Journal of Business Research*, 2023.



- [18] M. V. Mechelen, R. C. Smith, M.-M. Schaper, M. Tamashiro, K.-E. Bilstrup, M. Lunding, M. G. Petersen and O. S. Iversen, “Emerging Technologies in K–12 Education: A Future HCI Research Agenda,” in *ACM Transactions on Computer-Human Interaction*, 2023.
- [19] M. M. Mariani, I. Machado, V. Magrelli and Y. K. Dwivedi, “Artificial intelligence in innovation research: A systematic review, conceptual framework, and future research directions,” *Technovation*, 2023.
- [20] M. Santana and M. Díaz-Fernández, “Competencies for the artificial intelligence age: visualisation of the state of the art and future perspectives,” *Review of Managerial Science*, 2022.
- [21] T. K. Chiu, X. Z. Qi Xia, C. S. Chai and M. Cheng, “Systematic literature review on opportunities, challenges, and future research recommendations of artificial intelligence in education,” *Computers and Education: Artificial Intelligence*, 2023.
- [22] H. Crompton and D. Burke, “Artificial intelligence in higher education: the state of the field,” *International Journal of Educational Technology in Higher Education*, 2023.
- [23] ENISA, “Artificial Intelligence and Cybersecurity Research,” 2023.
- [24] The European Commission, “European Skills, Competences, Qualifications and Occupations (ESCO),” [Online]. Available: <https://esco.ec.europa.eu/en>.
- [25] European Committee for Standardization (CEN), “European e-Competence Framework (e-CF),” [Online]. Available: <https://ecfexplorer.itprofessionalism.org/>.
- [26] ENISA, “Addressing Skills Shortage and Gap Through Higher Education,” 2021.
- [27] J. Soldatos, “The EU-IoT Framework for Internet of Things Skills: Closing the Talent Gap,” 2023.
- [28] Frost & Sullivan, “European Cybersecurity Responsibility, Spending, and Posture: a Survey of Enterprise End Users Who Influence Cybersecurity Budgets.,” 2022.
- [29] Frost & Sullivan, “Global Digital Smart Borders Growth Opportunities: defining Future Growth Strategies for Different Ports of Entry.,” 2022.
- [30] Frost & Sullivan, “Top 20 Companies Accelerating Digital Transformation in the Global Waste Recycling and Circular Economy Industry: new Era of Data-driven Operation and Industry Convergence will Optimize Waste Services and Close the Loop on Material Sourcing.,” 2022.
- [31] Frost & Sullivan, “Global Artificial Intelligence Growth Opportunities: transformative Mega Trends in AI Create ICT Growth.,” 2022.
- [32] Frost & Sullivan, “Enhancing European Customer Experience with Artificial Intelligence: AI Technologies Offer New Opportunities to Nurture Relationships and Enhance Customer Contact Effectiveness.”.
- [33] Frost & Sullivan, “Technology Convergence is Enabling the Automotive Internet of Things (IoT): advanced Communication Technologies will Revolutionize Automotive IoT.,” 2022.
- [34] Frost & Sullivan, “IoT Cybersecurity Analysis—Blockchain-enabled IoT Cybersecurity Market: implementing New Service Models through Distributed Ledger Technologies,” 2018.
- [35] ENISA, “RESEARCH AND INNOVATION BRIEF: Annual Report on Cybersecurity Research and Innovation,” 2022.
- [36] CLUSIT, “Rapporto Clusit 2022,” 2022.
- [37] GARTNER, “Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026,” 2023. [Online]. Available: <https://www.gartner.com/en/newsroom/press->



releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026.

- [38] GARTNER, “Gartner Identifies Three Factors Influencing Growth in Security Spending,” 2022. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i>.
- [39] GARTNER, “Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23,” 2022.
- [40] GARTNER, “Gartner Identifies Top Five Trends in Privacy Through 2024,” 2022.
- [41] Expert Group on Future Skills Needs, “AI Skills: A Preliminary Assessment of the Skills Needed for,” 2022.
- [42] World Economic Forum, “The Future of Jobs Report,” 2020.
- [43] B. Marr, “What Are The Most In-Demand AI Skills?,” 2022. [Online]. Available: <https://www.forbes.com/sites/bernardmarr/2022/06/13/what-are-the-most-in-demand-ai-skills/?sh=37e038af249c>.
- [44] Internet of Learning, “13 Best Artificial Intelligence Bootcamps,” 2023. [Online]. Available: <https://internetoflearning.org/bootcamps/best-artificial-intelligence-bootcamps/>.
- [45] Coursera, “What Is an AI Engineer? (And How to Become One),” 2022. [Online]. Available: <https://www.coursera.org/articles/ai-engineer>.
- [46] Microsoft, “Learning paths and modules (queried with a specific subject and roles),” [Online]. Available: <https://learn.microsoft.com/en-us/training/browse/?roles=ai-engineer%2Cdata-engineer%2Cdata-scientist%2Cdeveloper%2Cfunctional-consultant&subjects=data-ai>.
- [47] European Technology and Innovation Platform, “Strategic Research and Innovation Agenda 2023,” 2023.
- [48] I. Campos, “What Does a Prompt Engineer Do?,” 2023. [Online]. Available: <https://medium.com/sopmac-ai/what-does-a-prompt-engineer-do-f00c6f2ad1ab>.
- [49] Gartner, “Roles and Skills to Support Advanced Analytics and AI Initiatives,” 2022.
- [50] CLUSIT, “Rapporto Clusit 2023,” 2023.
- [51] Gartner, *2022-2024 Technology Adoption Roadmap for Midsize Enterprises*, 2022.
- [52] McKinsey & Company, “The top trends in tech,” 2022.
- [53] C. Zhang and Y. Lu, “Study on artificial intelligence: The state of the art and future prospects,” *Journal of Industrial Information Integration*, 2021.
- [54] M. Sonia, “Top 3 Data Job Roles Explained : A Career Guide,” 2021. [Online]. Available: <https://www.ibm.com/blogs/ibm-training/top-3-data-roles-a-career-guide/>.
- [55] C. Keith, “Ethics and AI: Skills Needed,” 2018. [Online]. Available: <https://www.linkedin.com/pulse/ethics-ai-skills-needed-keith-cotterill>.
- [56] M. Benotmane, K. Elhari and A. Kabbaj, “A review & analysis of current IoT maturity & readiness models and novel proposal,” in *Scientific African*, 2023.



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:

- CS-Q1. "Monitoring" AND "large-scale" AND "security" AND ("complex systems" OR "anomalies" OR "performance" OR "threats").
- CS-Q2. "Threat modelling".
- CS-Q3. "Zero Trust".
- CS-Q4. "Risk management" AND "governance" AND ("mitigations" OR "ethic" OR "legal" OR "law").
- CS-Q5. "Machine learning" AND "context awareness".
- CS-Q6. "DevSecOps".
- CS-Q7. "Security Orchestration Automation and Response".
- CS-Q8. "security" AND ("Cloud computing" OR "mobile application" OR "api management").
- CS-Q9. "Incident management".
- CS-Q10. "artificial intelligence" AND "cybersecurity".
- CS-Q11. "Penetration testing".
- CS-Q12. "security" AND ("protocol" AND "secure transmissions" AND "secure channel" AND "cryptography").
- CS-Q13. "Multi-factor authentication" OR "conditional access control" OR "Behavioral authentication".
- CS-Q14. "Personal data protection".

Artificial intelligence domain:

- AI-Q1. "Artificial intelligence" AND ("Machine learning" OR "Ethical issues" OR "Knowledge representation" OR "knowledge reasoning" OR "Large Language Models" OR "Explainable AI").
- AI-Q2. "Generative AI tools" OR "Cyber AI" OR "Secure AI systems" OR ("artificial intelligence" AND "software") OR ("artificial intelligence" AND "algorithm design") OR ("Artificial Intelligence" AND "Secure systems") OR ("Artificial Intelligence" AND "software development") OR ("Artificial Intelligence" AND "algorithm design") OR ("Artificial Intelligence" AND "critical thinking") OR ("Artificial Intelligence" AND "analysis") OR ("Artificial Intelligence" AND "Complex problem solving") OR ("Artificial Intelligence" AND "active learning") OR ("Artificial Intelligence" AND "Machine learning technologies").
- AI-Q3. "Artificial intelligence" AND ("data quality" OR "big data" OR "data processing").
- AI-Q4. "Artificial intelligence" AND ("big data" OR "data science" OR "data processing").
- AI-Q5. "Artificial intelligence" AND "tool" AND ("reasoning" OR "design" OR "programming").
- AI-Q6. "Artificial intelligence" AND ("testbed" OR "co-development" OR "problem-solving").
- AI-Q7. "Artificial Intelligence" AND ("chatbot" OR "marketing" OR "higher education" OR "manufacturing" OR "space industry" OR "spatial data processing").
- AI-Q8. "Artificial Intelligence" AND ("education" OR "human-AI" OR "workplace well-being" OR "society well-being" OR "occupational well-being" OR "autonomous driving" OR "business management") OR ("digital marketing" AND "cloud").
- AI-Q9. "Artificial Intelligence" AND "adoption index".

Internet of things domain:

- IoT-Q1. "IoT" AND ("Azure" OR "AWS" OR "Google") OR ("service-oriented applications" OR "data ecosystems" OR "data spaces" OR "edge analytics" OR "cloud computing" OR "edge computing" OR "fog computing").
- IoT-Q2. "IoT" AND ("protocol" OR "DDS" OR "COAP" OR "AMQP" OR "MQTT" OR "MQTT-SN" OR XMPP" OR "COAP" OR "6LOWPAN" OR "LTE-A" OR "EPCglobal" OR "Z-Wave").
- IoT-Q3. "IoT" AND ("machine learning" OR "artificial intelligence" OR "TinyML" OR "cyber-physical systems" OR "big data" OR "distributed systems").
- IoT-Q4. "IoT" AND ("authentication" OR "Access control").
- IoT-Q5. "IoT" AND ("smart home" OR "smart transportation" OR "smart industry" OR "smart environment" OR "digital twins" OR "intelligent sensors" OR "real-time monitoring").
- IoT-Q6. "IoT" AND ("industry" OR "energy industry" OR "healthcare" OR "cellular IoT" OR "smart cars" OR "smart cities" OR "smart home" OR "smart grid").



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:
 - Send a request to a local server with the keyword.
 - Parse the response and extract the results.
 - For each result, check if it matches the keyword.
 - If it does, add any associated occupations to a global list.
 - Determine the type and parent of the keyword based on the result data.
 - 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.