Tackling Key Challenges of AI Development – Insights from an Industry-Academia Collaboration

Alexander Melde[1], Manav Madan[3], Paul Gavrikov[2], David Hoof[2], Astrid Laubenheimer[1], Janis Keuper[2], and Christoph Reich[3]
[1] Karlsruhe University of Applied Sciences, [2] Offenburg University, [3] Furtwangen University

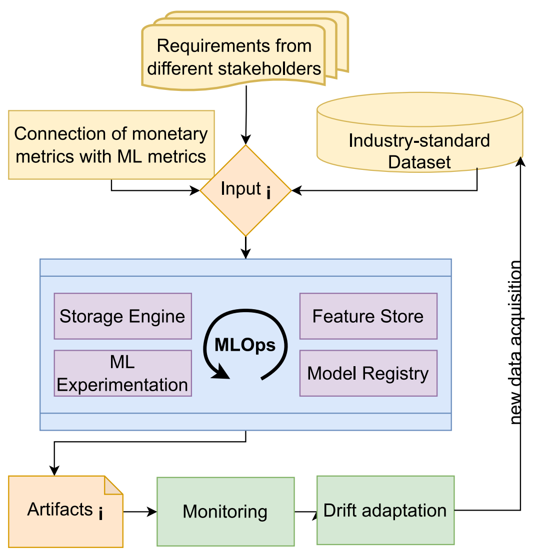
MOTIVATION

Harnessing the overall benefits of the latest advancements in artificial intelligence (AI) requires extensive **collaborations of academia and industry** – promoting innovation and growth while enforcing the practical usefulness of newer technologies in real life.

Challenges faced during these cross-collaborations are inspected with the help of the project *Q-AMeLiA**, in which three universities cooperate with five industry partners to **make the product risk of AI-based products visible**. The transformation of machine learning (ML) from academia to industry should be robust, simple and safe.

While big companies hire their own research teams, small and medium enterprises often rely on these cooperations in order to successfully adopt AI in their businesses.

FIGURE 1: MLOps Workflow



* This work was funded by the Ministry of Science, Research and Arts of Baden-Württemberg (MWK) as part of the project "Quality Assurance of Machine Learning Applications" (Q-AMeLiA).

GENERAL CHALLENGES

VARYING MINDSETS & CONFLICTS OF INTEREST

- different backgrounds and objectives
- standardization of concepts vs. algorithm breakthroughs
- uncertain return of investment for long-term research projects

OWNERSHIP OF INTELLECTUAL PROPERTY AND LEGAL REQUIREMENTS

- commerciality & open sourcing
- difference in regulations when results from academia shall be used in industry, e.g. for dataset licensing

DATA QUALITY AND QUANTITY

- good data vs. big data
- domain shift

OVERCHOICE IN SOURCE MODELS

- variety of pretrained models

INTEGRATION IN LEGACY SYSTEMS

- interoperability & efficiency
- choosing deployment infrastructure

ETHICAL CONCERNS

- fairness vs. short-term business value
- minimizing bias, ensuring explainability

TECHNICAL CHALLENGES

- lack of mature MLOps frameworks
- lack of uniformity in cloud solutions
- lack of common standards and metrics
- memory and resource limitations
- deployment & transferability
- gap in documentation between research and applied machine learning (ML)

DOMAIN SPECIFIC CHALLENGES

VISION-BASED ANOMALY DETECTION

- data versioning for images
- image quality estimation metrics
- occurrence of drifts
- lack of domain knowledge integration
- different spatial scales & aspect ratios
- speed vs. real-time dilemma

HARDWARE BENCHMARKING FOR ML

- lack of industry representative data
- lack of representative benchmarks
- lack of uniform metrics in benchmarks
- rapid growth
- domain dependency (task, dataset, …)
- scalability after hardware selection

CONTINUAL LEARNING UNDER DRIFT

- requirement of adaptable framework
- occurrence of drifts
- hyperparameter adaption (zero shot AutoML)
- catastrophic forgetting

INDUSTRIAL PROCESS AUTOMATION

- humongous unlabeled data (data collection)
- data quality estimation
- requirement of adaptable framework
- occurrence of drifts
- hyperparameter adaption (zero shot AutoML)
- interoperability challenges

SITUATION ANALYSIS (IN HEALTH CARE)

- video quality & camera conditions
- data collection & content complexity
- inconsistent definition of classes
- lack of mature framework
- occurrence of drifts
- lack of representative benchmarks

PROPOSED SOLUTIONS

GENERAL SOLUTIONS

- try to identify common interests
- track bottlenecks in ML workflows for continual improvement in production
- regulate AI systems to tackle ethical concerns
- encourage bi-directional exchange of talents between universities and industry
- identify new research directions and curriculums of universities based on problems encountered in the industry
- train students how to tackle applied real world challenges based on both knowledge learned in the industry and theoretical foundations.
- develop domain specific solutions with the help of industrial partners expertise

AUTOMATION, MLOPS & DRIFT ADAPTION

- perform tests and update deployed models continuously to counter drifts, e.g. via automated MLOps workflows (see figure 1)
- introduce tests and CI/CD patterns to increase scalability and reliability

DATA COLLECTION & QUALITY ESTIMATION

- introduce integrity checks to prove data is still in a known distribution
- detect outliers and handle missing values
- define what *good* data is in your use case
- involve domain expertise for higher quality labels, extend feedback loops between annotators and experts
- observe and track labeling mistakes
- evaluate the quality of your dataset on multiple dimensions (technical & ethical)

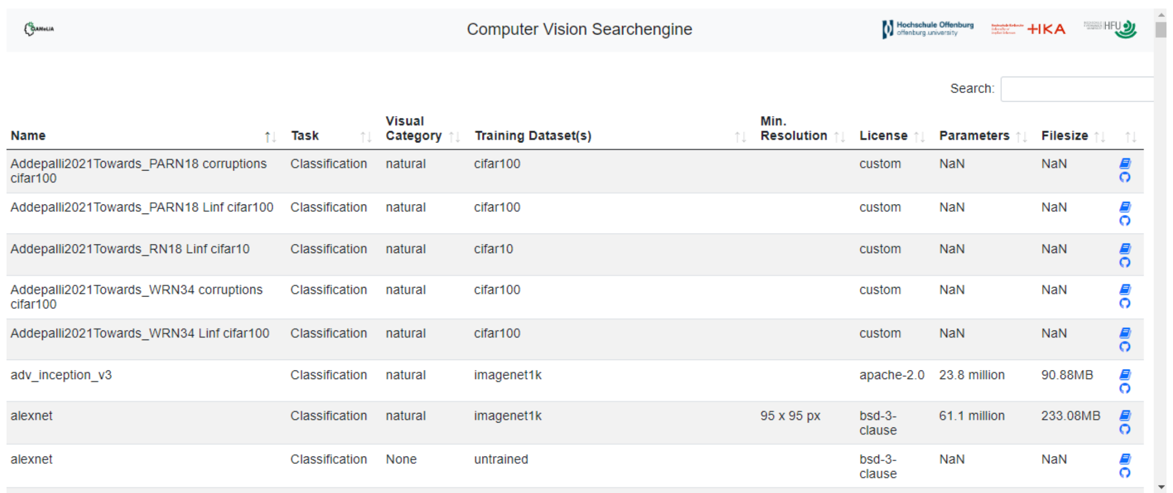
Q-AMELIA SEARCH ENGINE

- apply transfer learning to improve model quality without requiring further data
- use tools to help discover appropriate pretrained models, e.g. the Q-AMeLiA search engine developed during this work (see figure 2)

Open Q-AMeLiA Search Engine >

View Full-text article >

FIGURE 2: Q-AMeLiA Search Engine


Computer Vision Searchengine

Search:

Name	Task	Visual Category	Training Dataset(s)	Min. Resolution	License	Parameters	Filesize
Addepalli2021Towards_PARN18 corruptions cifar100	Classification	natural	cifar100		custom	NaN	NaN
Addepalli2021Towards_PARN18 Linf cifar100	Classification	natural	cifar100		custom	NaN	NaN
Addepalli2021Towards_RN18 Linf cifar10	Classification	natural	cifar10		custom	NaN	NaN
Addepalli2021Towards_WRN34 corruptions cifar100	Classification	natural	cifar100		custom	NaN	NaN
Addepalli2021Towards_WRN34 Linf cifar100	Classification	natural	cifar100		custom	NaN	NaN
adv_inception_v3	Classification	natural	imagenet1k		apache-2.0	23.8 million	90.88MB
alexnet	Classification	natural	imagenet1k	95 x 95 px	bsd-3-clause	61.1 million	233.08MB
alexnet	Classification	None	untrained		bsd-3-clause	NaN	NaN