

REGULATION-AWARE SOFTWARE ARCHITECTURE

Rise of AI/ML techniques and emerging regulations have added further complexity in the software engineering domain. Software engineering practitioners, in particular those working on software design and architecture practices must take these new technologies and regulations in their daily work. This calls for additional considerations as part of many technical activities. Our vision addresses the challenges posed by emerging technologies, new regulations, and the concerns behind the regulations.



Ali Mehraj
ali.mehraj@tuni.fi
Tampere University

Supervisors:
Kari Systä
David Hästbacka

MOTIVATION

- Difficulty in representing regulations in software architecture description.
- Lack of representation tools of AI/ML models in software architecture description.
- Limitation in running analysis on the validity of a software architecture, especially in terms of regulations.

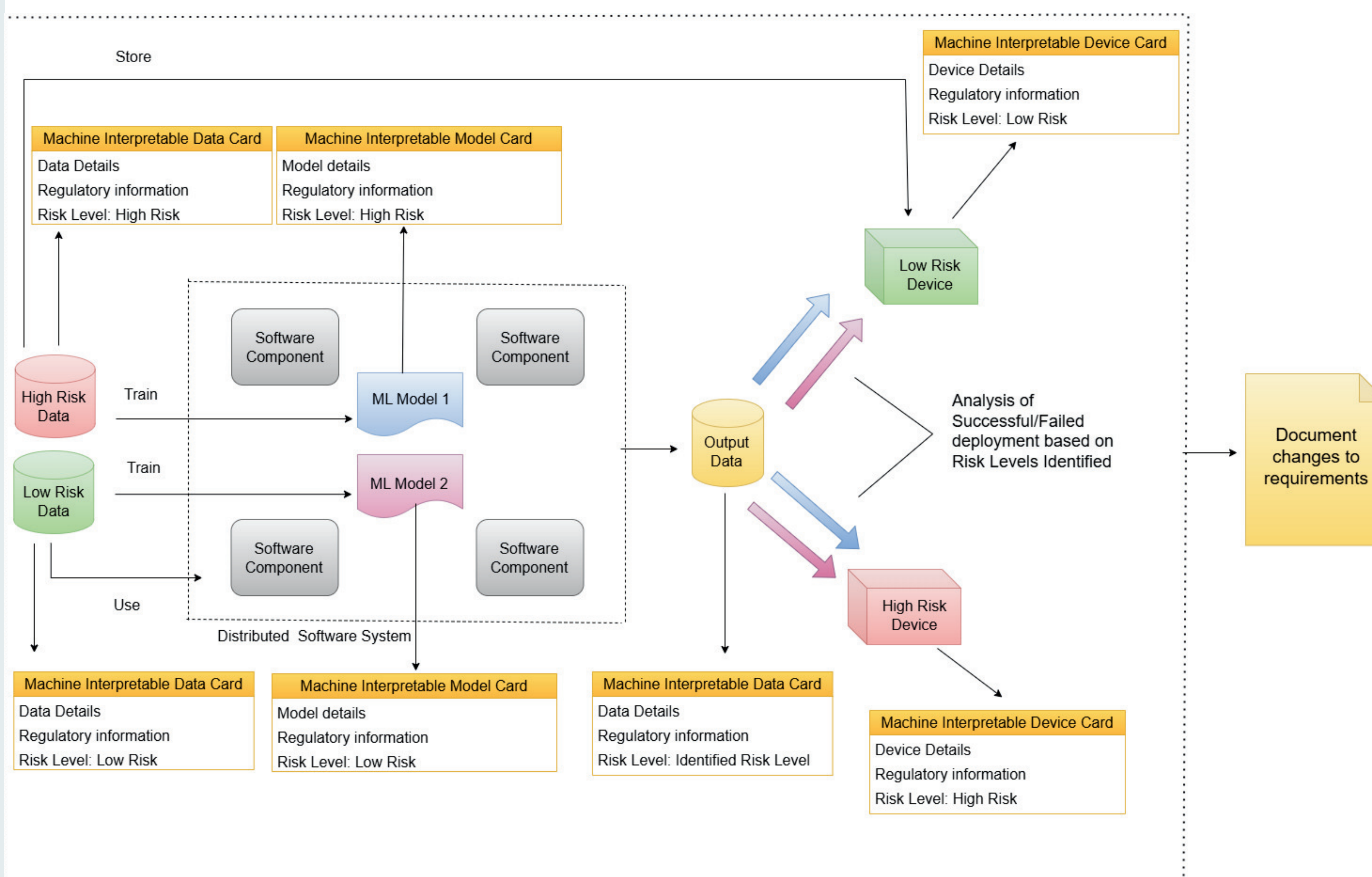
CORE OBJECTIVES

- Develop methods to incorporate regulations in architecture description.
- Develop methods to analyze the properties of the architecture.
- Develop methods to validate regulatory compliance.

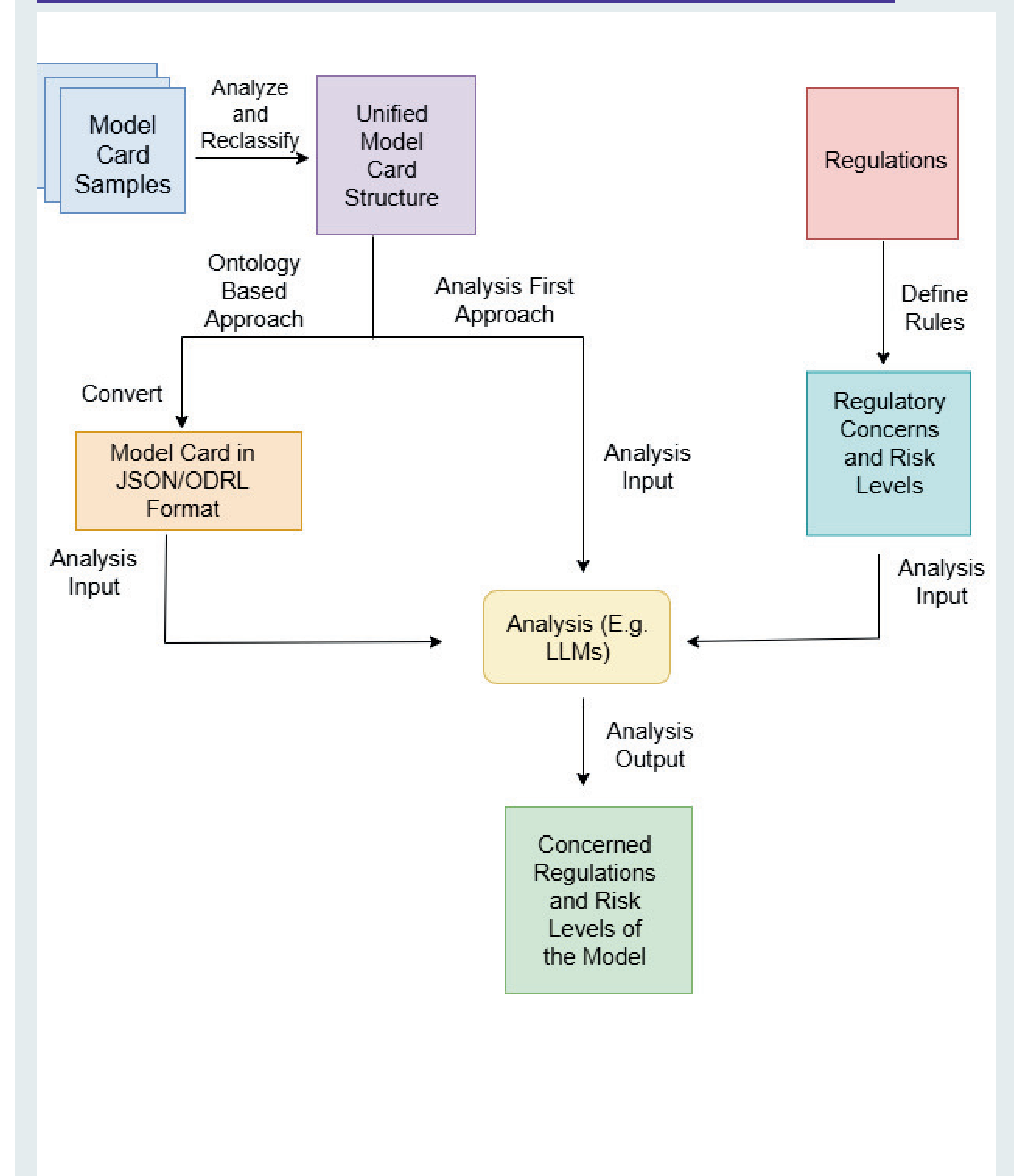
RESEARCH QUESTIONS

- RQ1. How can we represent regulatory concerns (EU AI Act, GDPR) in software architecture description?
- RQ2. How can we analyze the properties of the architecture for regulatory compliance?
- RQ3. How can we validate regulatory compliance in a software system?

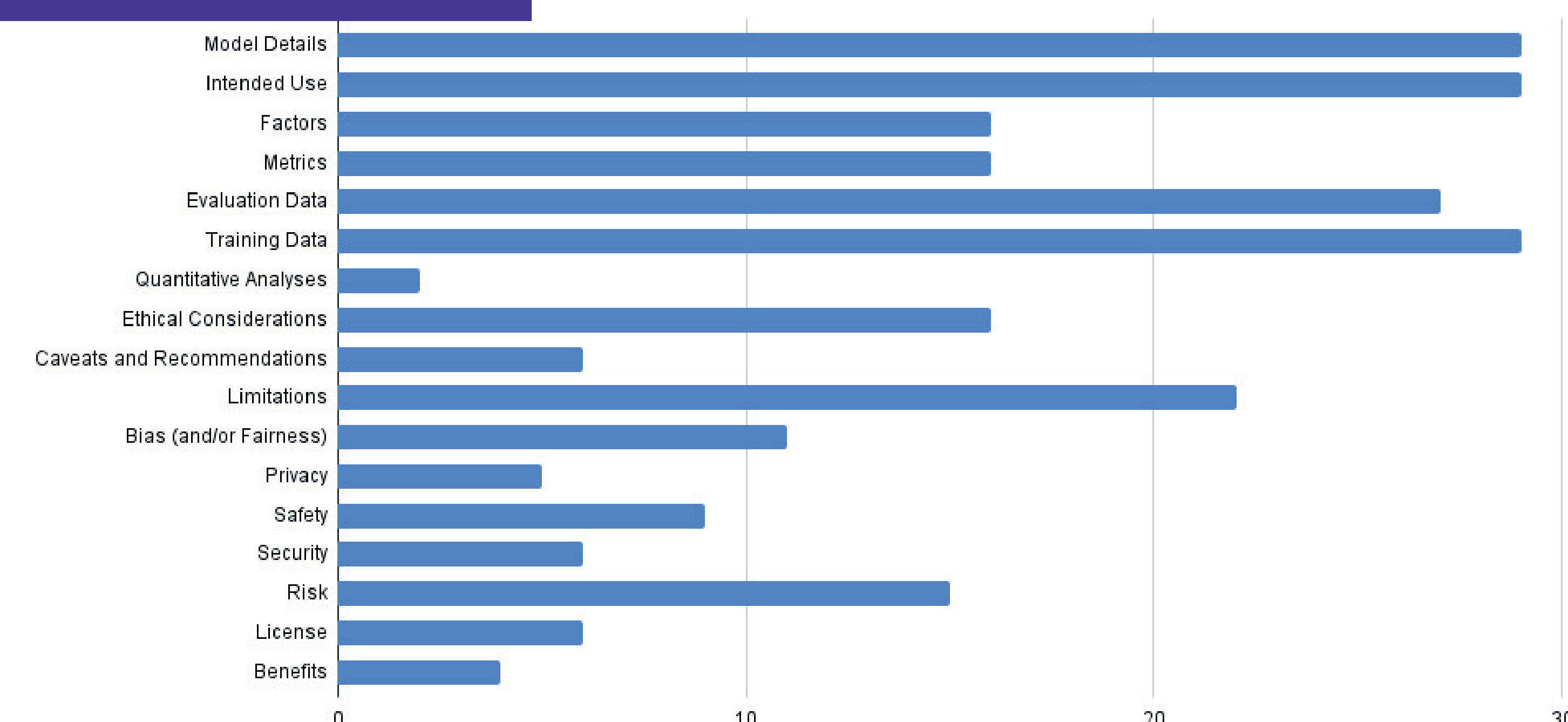
THE VISION



MODEL CARD DATA EXTRACTION



ONGOING RESEARCH



Model Cards	Organization
Claude 2, Claude 3	Anthropic
Stable Diffusion	CompVis
Gopher	DeepMind (Google)
Gemma 2, CodeGemma, PaliGemma, RecurrentGemma, MedLM, PaLM, FaceMesh, Gemini 1.0, Gemini 1.5	Google
Llama 2, Llama 3, AudioCraft, MusicGen, Galactica	Meta
PeopleNet, DashCamNet, FaceDetectir, VehicleTypeNet, TrafficCam-Net	Nvidia
GPT-2, GPT-3, GPT-4, CLIP, DALLE-2	OpenAI
CTRL	Salesforce

NEXT STEPS

- Establish a high-quality unified model card structure.
- Develop methods to define rules for regulatory concerns and risk levels
- Develop methods to extract regulatory concerns and risk levels from the model cards.
- Methods to incorporate metadata cards in the software architecture description.

RELATED PUBLICATIONS

- Kotilainen, P., Mäkitalo, N., Systä, K., Mehraj, A., Waseem, M., Mikkonen, T., Murillo, J.M.: Allocating distributed ai/ml applications to cloud-edge continuum based on privacy, regulatory, and ethical constraints. *Journal of Systems and Software* 222, 112333 (2025).
- Kotilainen, P., Mehraj, A., Mikkonen, T., Mäkitalo, N.: The programmable world and its emerging privacy nightmare. In: *International Conference on Web Engineering*. pp. 255–262. Springer (2024)
- Akbar, M.A., Esposito, M., Hyrynsalmi, S., Kumar, K.D., Lenarduzzi, V., Li, X., Mehraj, A., Mikkonen, T., Moreschini, S., Mäkitalo, N., Oivo, M., Paavonen, A.S., Parveen, R., Smolander, K., Su, R., Systä, K., Taibi, D., Yang, N., Zhang, Z., Zohaib, M.: 6GSoft: Software for Edge-to-Cloud Continuum. *SEAA 2024*: 499-506.
- Mehraj, A., Zhang, Z., Systä, K.: A Tertiary Study on AI for Requirements Engineering. In: *International Working Conference on Requirements Engineering: Foundation for Software Quality*. pp. 159–177. Springer (2024)