AI-VuTeP

Kimmo Halunen
University of Oulu, Finland

Idea

- To develop a platform for testing, finding, reporting and fixing AI security and privacy vulnerabilities.

Market relevance

- AI systems need to be trustworthy and robust in order to be acceptable to the users
- Also regulation on the transparency and accountability on AI systems
- Finding and fixing potential vulnerabilities earlier in the prodcut lifecycle will lead to faster and better AI systems

Innovation

- Developing a framework and a platform that can be used to test AI systems and algorithms for security and privacy vulnerabilities
- Also new methods to report the found issues to relevant stakeholders in an ethical manner

Looking for

- Industry partners to test our platform in real use cases
- Research partners to work on the research questions
- Coordinator to lead the project OR a more ready project proposal where new ideas are welcome