Machine Learning

Timing: 1st year of study **Scope: 10** ECTS

Content: The purpose of the course is to introduce the student to Machine Learning, so that the student can develop applications by using some of the most common Machine Learning techniques and model architectures.

Learning objectives:

Knowledge

The student must have knowledge of:

- What Machine Learning is good for, and its limitations
- Several popular applications of Machine Learning
- Supervised, unsupervised and reinforcement learning
- The types of predictions that machine learning solutions can make, including regression as well as binary and multiclass classification
- A few of the most common Machine Learning model architectures, including artificial neural network
- The development process for Machine Learning applications
- Key issues after having trained a model, such as over- and underfitting
- Large language models (LLMs), their structure, capabilities and applications
- Available open source LLM frameworks and tools
- Design patterns used in AI agents

Skills

The student can:

- Develop Machine Learning applications that are based on supervised learning
- Develop a Machine Learning application using a deep learning neural network architecture, and at least one other model architecture that is not based on neural networks
- Use basic techniques for validation and fine-tuning of trained models
- Use basic techniques for data preparation
- Use at least one popular programming framework to develop Machine Learning applications
- Utilize existing frameworks to integrate with LLMs
- Implement AI agent capable of performing specific tasks autonomously
- Assess the performance of AI agents

Competencies

The student can:

- Compare different model architectures, and reason about which one will be best suited to solve a specific problem
- Design application features that are using machine learning models

The examination

Internal oral exam of 20 minutes duration based on a project.

Assessment

7-point grading scale. Grading is based on an overall assessment of the oral presentation and examination, but not on the submitted project.

Secure Software Development

Timing: 1st year of study **Scope: 10** ECTS

Content: The purpose of the course is to train the student in developing secure software systems with a focus on Security by Design. The student will be able to use applied cryptography and consider security as an integral part of all phases in the software development life cycle.

Learning objectives:

Knowledge

The student must have knowledge of:

- Key cryptographic primitives
- Federated authentication
- Common vulnerabilities and mitigation techniques
- Secure design principles
- Key EU cybersecurity legislation (e.g., CRA, GDPR, NIS2) at a non-expert, awareness level

Skills

The student can:

- Demonstrate practical application of cryptography (e.g. encryption, hashing)
- Design software systems with focus on security
- Understand and model threats
- Assess security posture of software systems
- Assess security implications in relation to supply chain of software

Competencies

The student can:

- Apply security measures and best practices throughout entire software development life cycle

The examination:

Internal oral exam of 20 minutes duration based on a project.

Assessment

7-point grading scale. Grading is based on an overall assessment of the oral presentation and examination, but not on the submitted project.