QuantifiCare

A.I. seminar

Challenges of A.I. : integrity, confidentiality and availability

Course presentation

Course execution (18h):

I) Lectures: 9 h
II) Practical courses: 2 x 3h
III) Project defense: 3h (for all groups)

Evaluation:

I) Each practical course will be graded (20% final grade)
II) Project defense (80% final grade)

Teacher:

Ph.D. in Machine Learning: integrity of neural networks against adversarial examples
Mail: rbernhard@quantificare.com

Course presentation

QuantifiCare

Goals of this course:

- Introduce and present industry relevant topics, such as **security** and **confidentiality**
  => Topics that **enhance your understanding of neural networks**

- **Implement** some concepts in practical courses

- Propose a project to go further and initiate yourself to scientific literature

Course presentation

QuantifiCare

Requirements

- Computer with Python + Deep Learning library of your choice (Tensorflow, Pytorch, Jax, etc.)
- Know how to install external libraries (conda, pip, etc.)

- Basic understanding of machine learning (training/inference, generalization gap, overfitting, etc.)
- Basic understanding of neural networks (back propagation, dense layers, convolutional layers, batch normalization, etc.)

Course presentation

Three main chapters

Mix of theory and practice

I) Overview of Adversarial Machine Learning

i) Adversarial context, Adversarial threat model

ii) Presentation of different types of attacks

II) Adversarial examples --- Practical course