Blekinge Institute of Technology
Department of Computer Science

Revision: 1
Reg.no: BTH-4.1.14-0826-2021

COURSE SYLLABUS

Maskininlärning och säkerhet

Machine Learning Security

6 credits (6 higher education credits)

Course code: DV2612
Main field of study: Computer Science, Software Engineering
Diciplinary domain: Technology
Education level: Advanced level
Specialization: A1N - Second cycle, has only first-cycle sourse/s as entry requirements

Language of instruction: The language of instruction is English.
Applies from: 2022-01-17
Approved: 2021-09-01

1. Decision

This course is established by Dean 2021-04-29. The course syllabus is approved by Head of Department of Computer Science 2021-09-01 and applies from 2022-01-17.

2. Entry requirements

Admission to the course requires at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).

3. Objective and content

3.1 Objective

The main objective of this course is to acquaint students with existing approaches, methods, and tools of machine Learning (ML) for security as well as unveil security issues in ML itself.

3.2 Content

This course is divided into the following two parts. First, it covers security problems in ML systems, e.g., showing various types of attacks on ML systems in an applied fashion-adversarial ML. Secondly, available methods, tools and other safeguards that could be used against the different types of attacks are covered.
The course includes both theoretical introductions to the different attack types and security-enhancing methods and tools, as well as more practical hands-on assignments in Python. After the course the student will have obtained the basic knowledge about security-enhancing approaches, and how to use them to protect against various risks in ML systems and how to use ML to detect cyber-attacks.

Main modules of this course are:
- Machine Learning Basics
- Security for Machine Learning
- Machine Learning for Security
- Applied Machine Learning

4. Learning outcomes

The following learning outcomes are examined in the course:

4.1 Knowledge and understanding

On completion of the course, the student will be able to:
- Discuss security aspects in machine learning and vice versa.
- Explain how to apply different ML methods and models for solving the security issues.
- Understand the basic principles of machine learning in security and reasons for its implementation.

4.2 Competence and skills

On completion of the course, the student will be able to:
- Apply ML tools, methods in processing the security data to extract new information out of it.

4.3 Judgement and approach

On completion of the course, the student will be able to:

• Evaluate the appropriate application of the ML tools and methods that are presented in the course to choose the best fit for their purposes.

5. Learning activities

The teaching is organised around online lectures, pre-recorded videos, together with written material, literature, and research literature. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through email and the course's online learning platform.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2205	Written assignment 1	1 credits	GU
2215	Written assignment 2	1 credits	GU
2225	Written assignment 3	2 credits	GU
2235	Written assignment 4	2 credits	GU

The course will be graded G Pass, UX Insufficient, supplementation required, U Fail.

The course-PM for each course revision should include the assessment criteria and make explicit in which modes of examination that the learning outcomes are assessed.

An examiner can, after consulting the Disability Advisor at BTH, decide on a customized examination form for a student with a long-term disability to be provided with an examination equivalent to one given to a student who is not disabled.

7. Course evaluation

The course evaluation should be carried out in line with BTH:s course evaluation template and process.

8. Restrictions regarding degree

The course can form part of a degree but not together with another course the content of which completely or partly corresponds with the contents of this course.

9. Course literature and other materials of instruction

Materials such as research articles and other course materials, as well as recommendations for additional reading, are provided via the courses' online platform.