Linnéuniversitetet
Linnaeus University

Thesis Topic	**Artificial Intelligence in Cyber-Security**
Motivation	In the Internet-of-Things (IoT, also known as the Internet-of-Everything, IoE) and Factory 4.0 era, the security of Internet-connected computer systems has become essential. However, the ever changing and complex nature of cyber-physical threats make them difficult to detect in real-world environments. Therefore, efforts should be aimed at developing future-proof frameworks, methodologies and tools that can quickly adapt to novel threat scenarios through artificial intelligence (AI) and machine learning.
Tasks	The thesis will address security risk management through suitable AI modeling languages, like Bayesian Networks (BN) and Artificial Neural Networks (ANN), in the context of on-line cyber-physical threat detection frameworks, with the aim of coping with large amount of events/states/actions, possibly including approaches based on UML, Semantic Models and Big Data Analytics. The student will be required to study, develop and evaluate AI methods/models in selected security applications and case-studies of industrial relevance.
Prerequisites *	Recommended courses, although not mandatory: - 4DV608 Advanced Software Design - 1DV200/1DV700 Computer Security Minimum grade average: C
We offer you	Preliminary meeting to clarify objectives and requirements. Support and study materials (slides, lecture notes, technical books, research papers, etc.) on cyber-security and artificial intelligence modeling paradigms. Artificial Intelligence (ANN, BN, etc.) modeling tools.
Time frame	-
Supervisor(s)	Dr. Francesco Flammini Senior Lecturer Department of Computer Science Faculty of Technology francesco.flammini@lnu.se

* All the course codes, like e.g. 1DV101, refer to courses here at DFM. Similar documented experience from other places will do just as well.