Machine Learning for Security Applications

Overview

- Description: Machine learning (ML) is a subtopic of artificial intelligence (AI)[1,2]. It is concerned with techniques that enable computers to automatically learn certain tasks from data, e.g. to recognize faces in images. In ML there is a training phase in which the computer learns from training data. With respect to the training phase, one can essentially differentiate between supervised learning (a computer is presented with example inputs and their desired outputs) and unsupervised learning (the learning algorithm is left alone to find structure in its input).
- State of research: Research in this area is steadily growing, e.g. due to more powerful hardware and big data. An important breakthrough was the development of Deep Learning, which is based on artificial neural networks (ANN)[3]. ANNs are a comparatively old approach to machine learning and are inspired, to some extent, by the neuroanatomical architecture of the brain.
- Capabilities: ML is regarded as a key technology for artificial intelligence. Application areas are e.g. pattern, image and voice recognition technologies, as well as pharmaceutical sciences (drug development) and material sciences (enhancement of material formulations).
- Limits: Currently, ML needs a lot of time and effort for training algorithms. If ML is to be used in decision making processes (such as finding a terrorist in a group of people) there are also important legal questions to answer. Especially in these cases ML needs to be very robust, which means that it gains the ability to get to the correct answer (almost) all the time.

Further Information

- Key player: Companies e.g. Google, Facebook, Microsoft, Apple or IBM and research institutes worldwide. In Europe e. g. DeepMind (UK).
- Readiness: The technologies for ML are in constant further development. At the moment, there is still no AI system that, like humans, can be used simultaneously for different tasks (General AI). Instead, current systems are tailor-made for their respective task (Narrow AI).
- Users: Universities, companies, military, security, health related institutions, emergency services, traffic control, space agencies, …
- Future outlook and foresight: Whether ML in its current form can make significant contributions to the development of a general AI in the future is not yet foreseeable. Such a universally applicable AI system is at the moment only to be expected in the very long term.
- Related Technologies: Artificial Intelligence, Data Mining, Big Data, hardware development
- Links: [1] BENGIO, Yoshua: Machines Who Learn. In: Scientific American 314 (2016), Nr. 6, S. 46–51, DOI: http://dx.doi.org/10.1038/scientificamerican0616-46; [2] JORDAN, M. I. ; MITCHELL, T. M.: Machine learning: Trends, perspectives, and prospects. In: Science 349 (2015), Nr. 6245, S. 255–260, DOI: http://dx.doi.org/10.1126/science.¬aaa8415; [3] LECUN, Yann ; BENGIO, Yoshua ; HINTON, Geoffrey: Deep learning. In: Nature 521 (2015), Nr. 7553, S. 436–444, DOI: http://dx.doi.org/10.1038/nature14539