Machine learning - Best practices and vulnerabilities

Sebastiano Galazzo
Sistem-evo, Italy

Artificial intelligence and machine learning are a must nowadays. For projects carrying a simple or well-known problem we can find a lot of ready-made solutions, but the game changes when facing with specific custom problems. The first part of this session is a deep down on techniques approaches and best practices in configuring ML algorithms but much more, do we really need it always? The second part will cover vulnerabilities of ML, discovering how easy could be to fool and to hack a neural network by some techniques (Like pixel attack) and their implication in (our) security. A demonstration will focus on a case of e-commerce using cloud ML (Cognitive) services, breaking them then possible solutions and workarounds.

Biography

Sebastiano Galazzo is an artificial intelligence researcher. Winner of two AI awards, he has been working in AI and machine learning for 20 years, designing and developing AI and computer graphic algorithms. Very passionate about AI, interested in technologies focused on image and natural language processing, and predictive analysis. He received several national and international awards that recognize his work and contributions in these areas.

Sebastiano.galazzo@gmail.com