Adversarial machine learning on classification tasks invented

Poisoning and evasion attacks and defenses of classification invented

Deep learning wins ImageNet Challenge

General adversarial networks (GANS) invented and a surge in adversarial examples

Adversarial attacks are prevalent and robustness issues are dominant

Verification for deep learning invented

Al interpretability proposed

2010 Rise of Al

Blowout Year for Al

2001 A deterministic method for verification used to verify the accuracy of simple neural networks

Deep learning (AlphaGo) wins world Go champion Lee Sedol

Deep neural networks are vulnerable

Safety issues of intelligent cyber-physical systems are emerging

2018 Testing for deep learning invented2018 Methods of adversarial examples generation are still hot