

Fooling deep neural net classifiers

Title: Universal adversarial perturbations

Authors: Moosavi-Dezfooli, Seyed-Mohsen; Fawzi, Alhussein; Fawzi, Omar; Frossard, Pascal

Publication: eprint arXiv:1610.08401 **Publication Date:** 10/2016



- It's an Indian elephant!
- At least after adding a universal noise to the image
- Deep learning models do not mimic brain activity

This is not a sock

Fooling deep neural net classifiers

Autonomous driving!



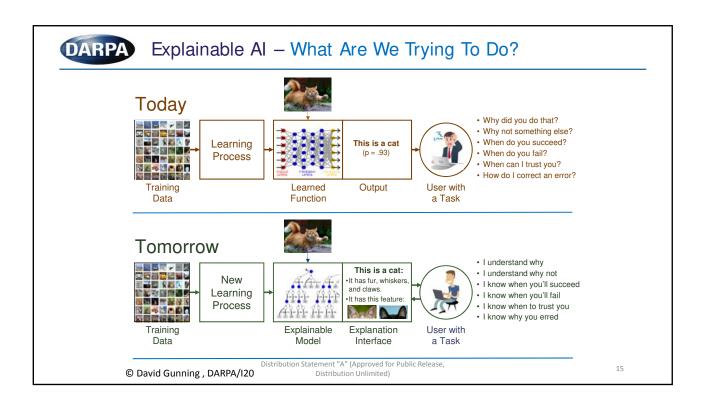


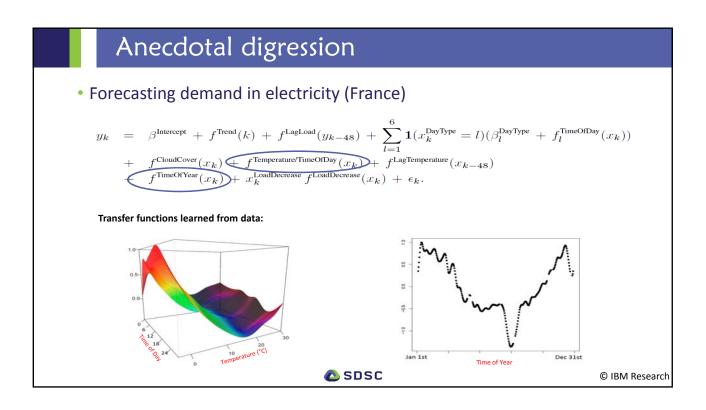


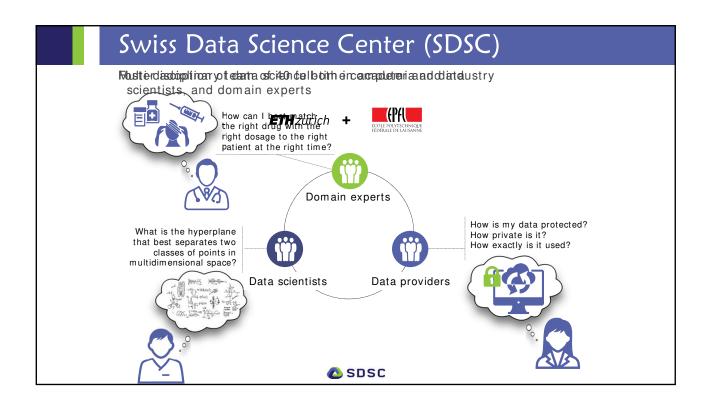
• Turning a STOP sign into a 45 mph speed limit

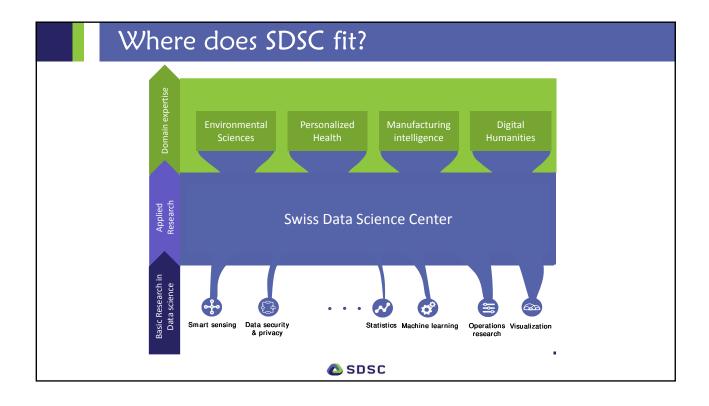


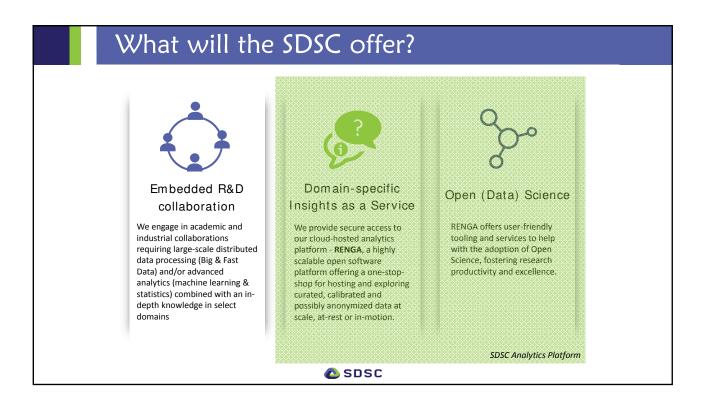
SDSC

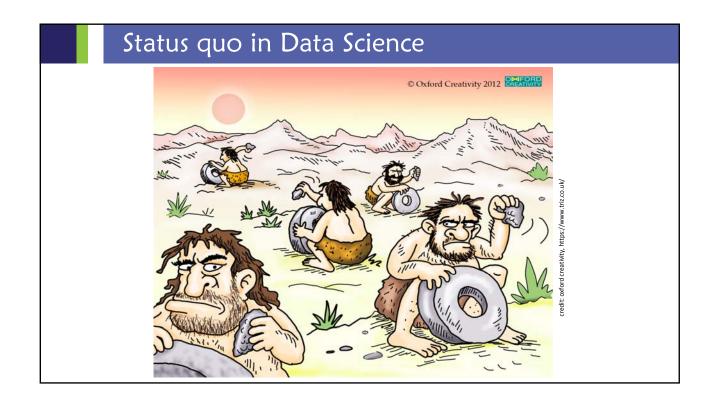


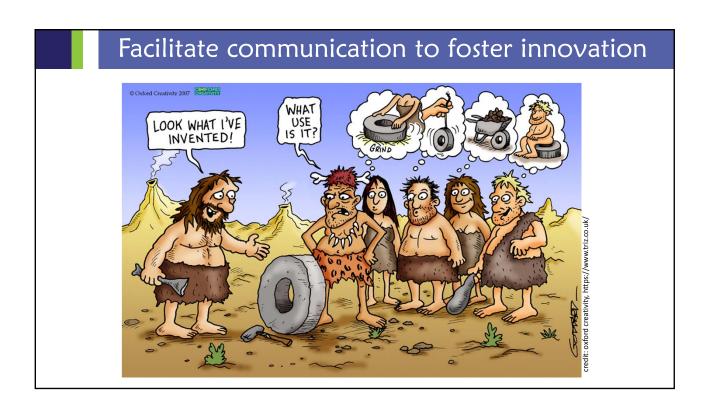




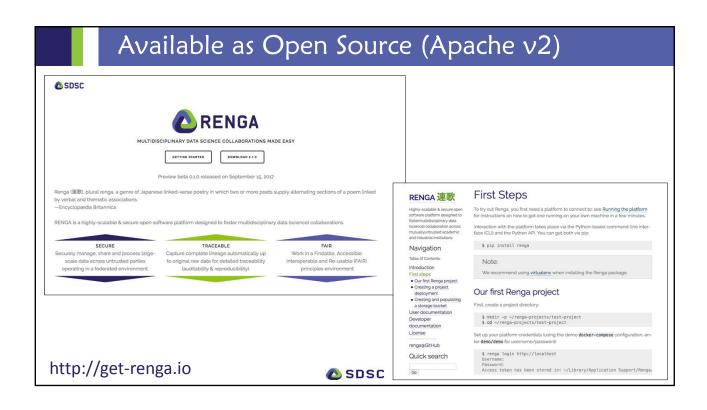














Objectives

- Understand why some of the company's best and most experienced employees are leaving prematurely
- 2. Predict which valuable employees will leave next

SDSC

Dataset published by IBM

- Fictitious large company
- 14,999 employees
- 10 data fields include:
 - Employee satisfaction level, scaling 0 to 1
 - Last evaluation, scaling 0 to 1
 - · Number of projects
 - Average monthly hours
 - Time spent at the company in years
 - · Whether they have had a work accident
 - Whether they have had a promotion in the last 5 years
 - Sales (which actually means job function)
 - · Salary low, medium or high
 - Whether the employee has left

SDSC

