Machine và Ứng Dụng

Vũ Đức Lý Phan Văn Tâm Nguyễn Hồng Tất

VSEC Lab

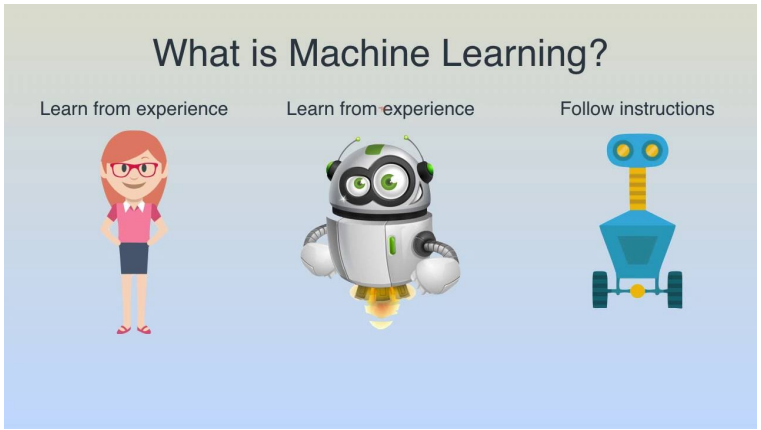
vseclab2017@gmail.com

Ngày 23 tháng 9 năm 2017

Overview

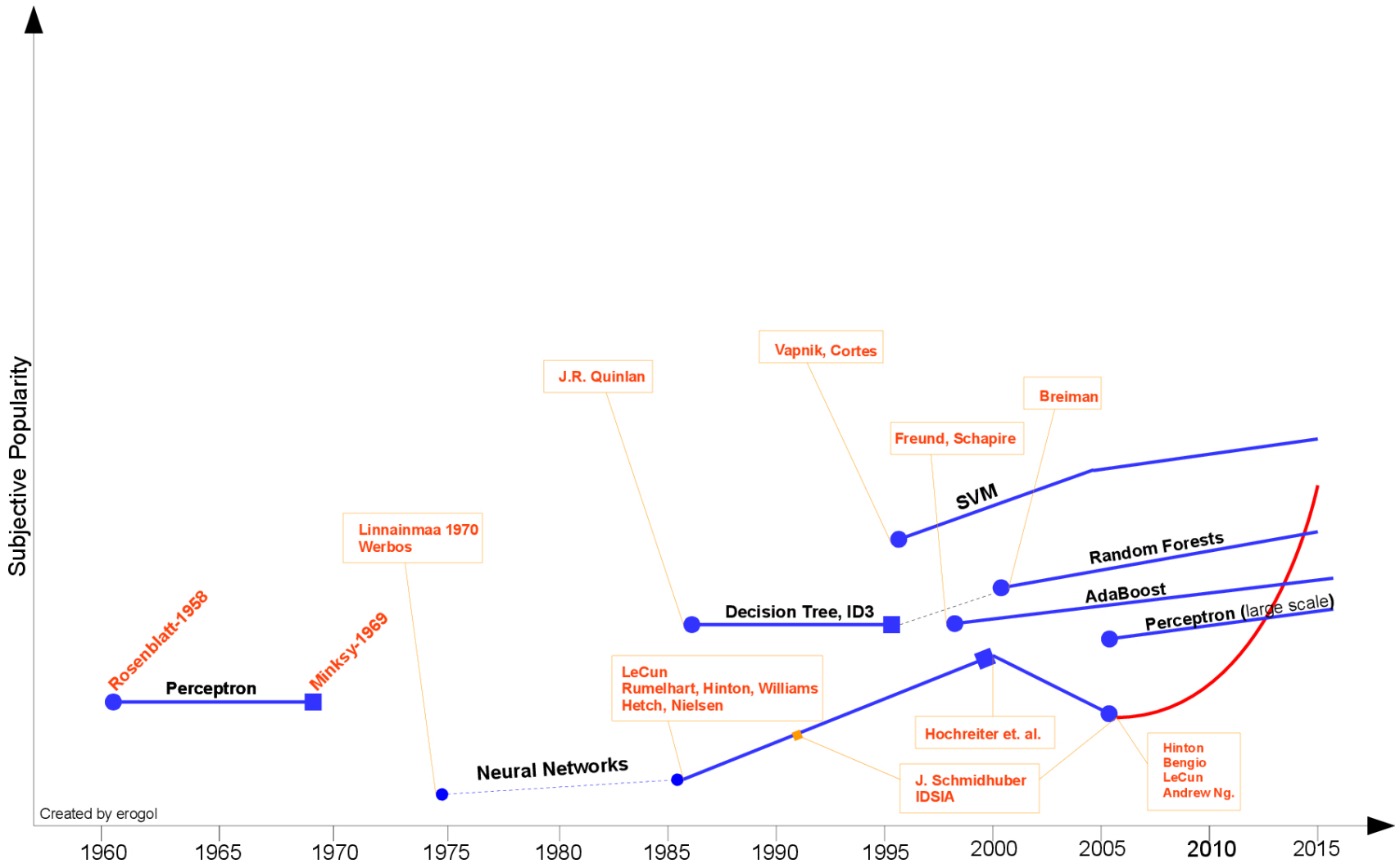
Định nghĩa

Là một lĩnh vực nhỏ của Khoa Học Máy Tính, nó có khả năng tự học hỏi dựa trên dữ liệu đưa vào mà không cần phải được lập trình cụ thể.



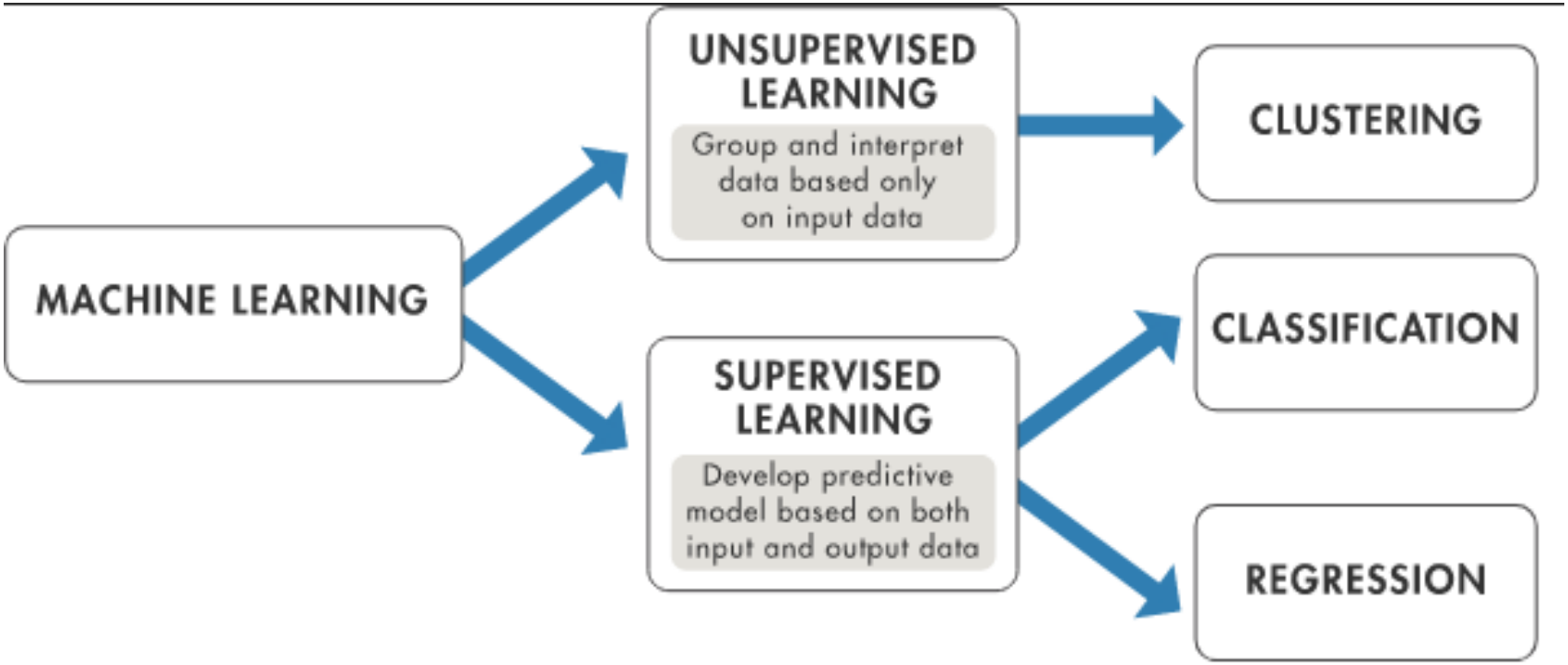
Hình: youtube.com

Lịch sử



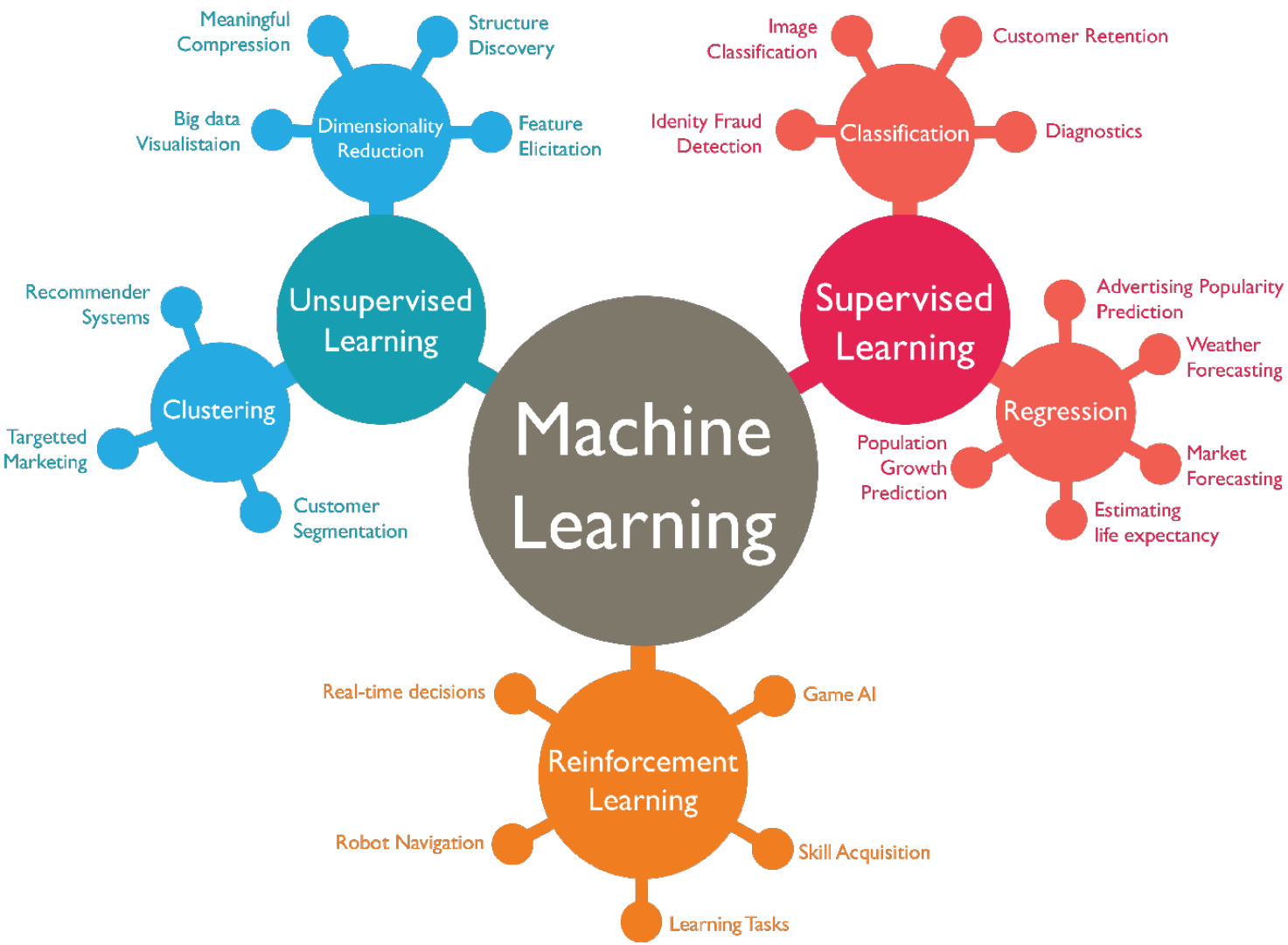
Hình: erogol.com

Kĩ thuật machine learning



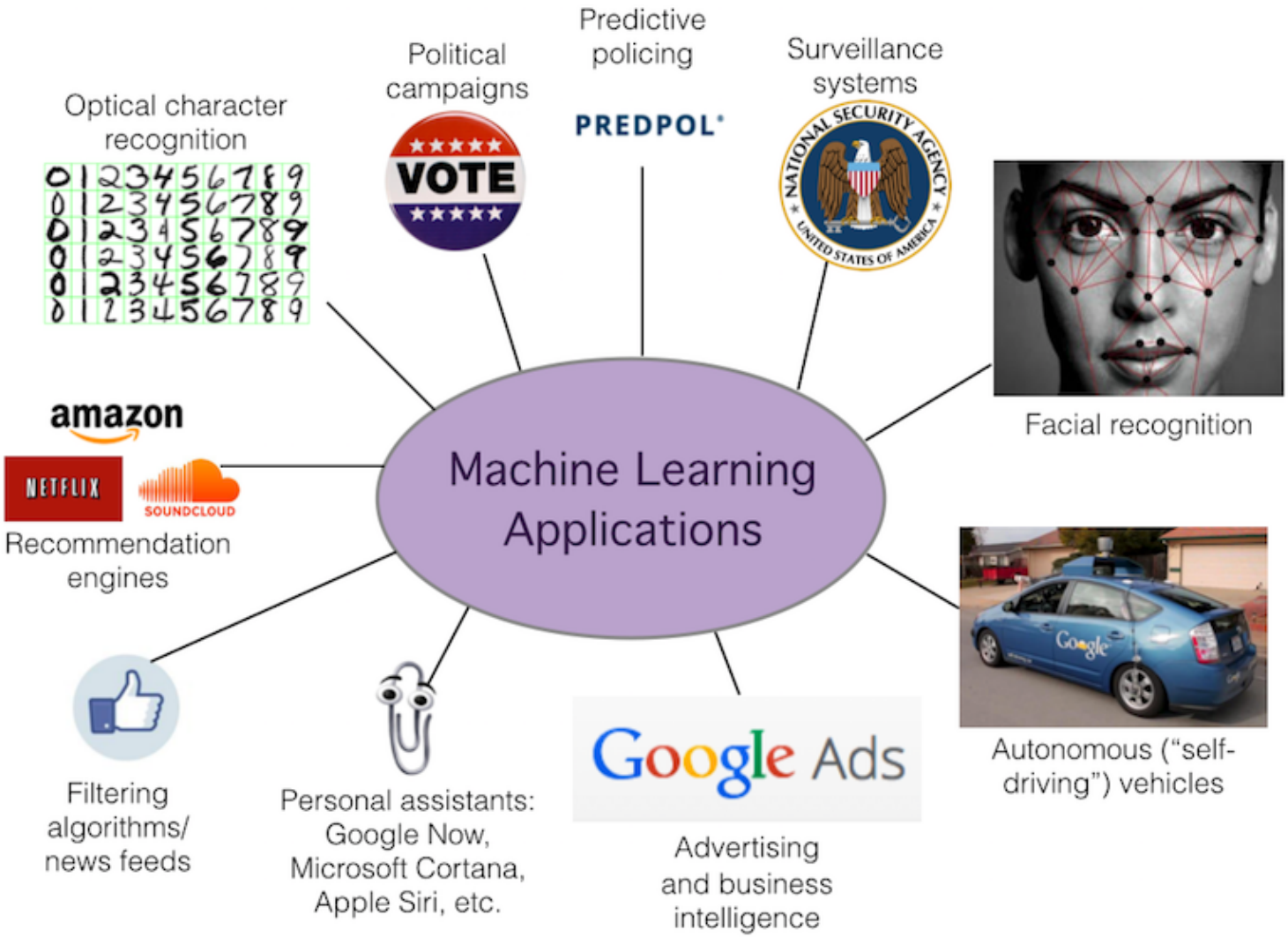
Hình: au.mathworks.com

Ứng dụng



Hình: Image via Abdul Rahid

Sử dụng hàng ngày

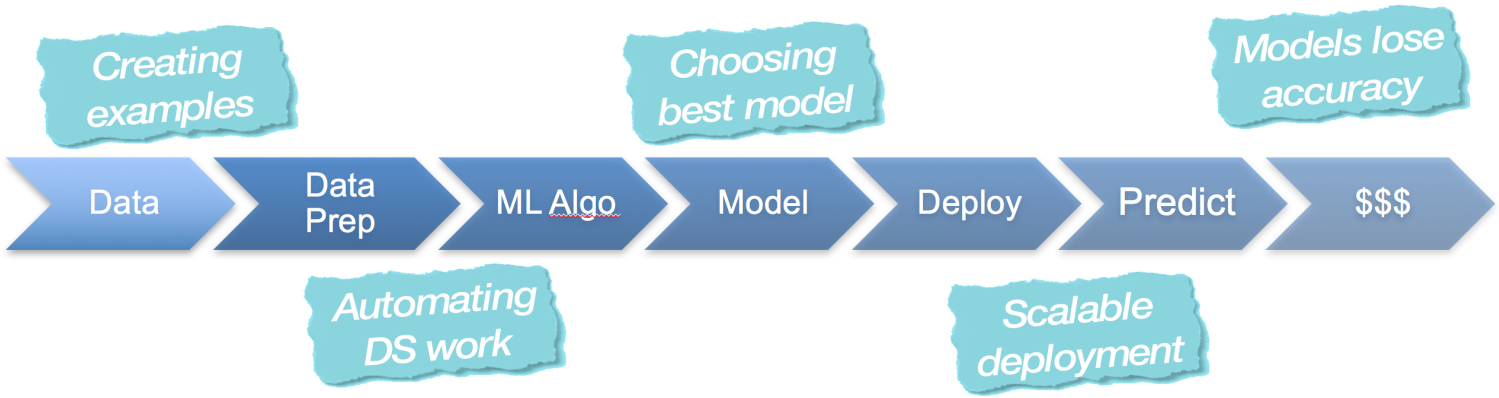


Hình: quora.com

Workflow

- **The Machine Learning Workflow**

- Not that simple

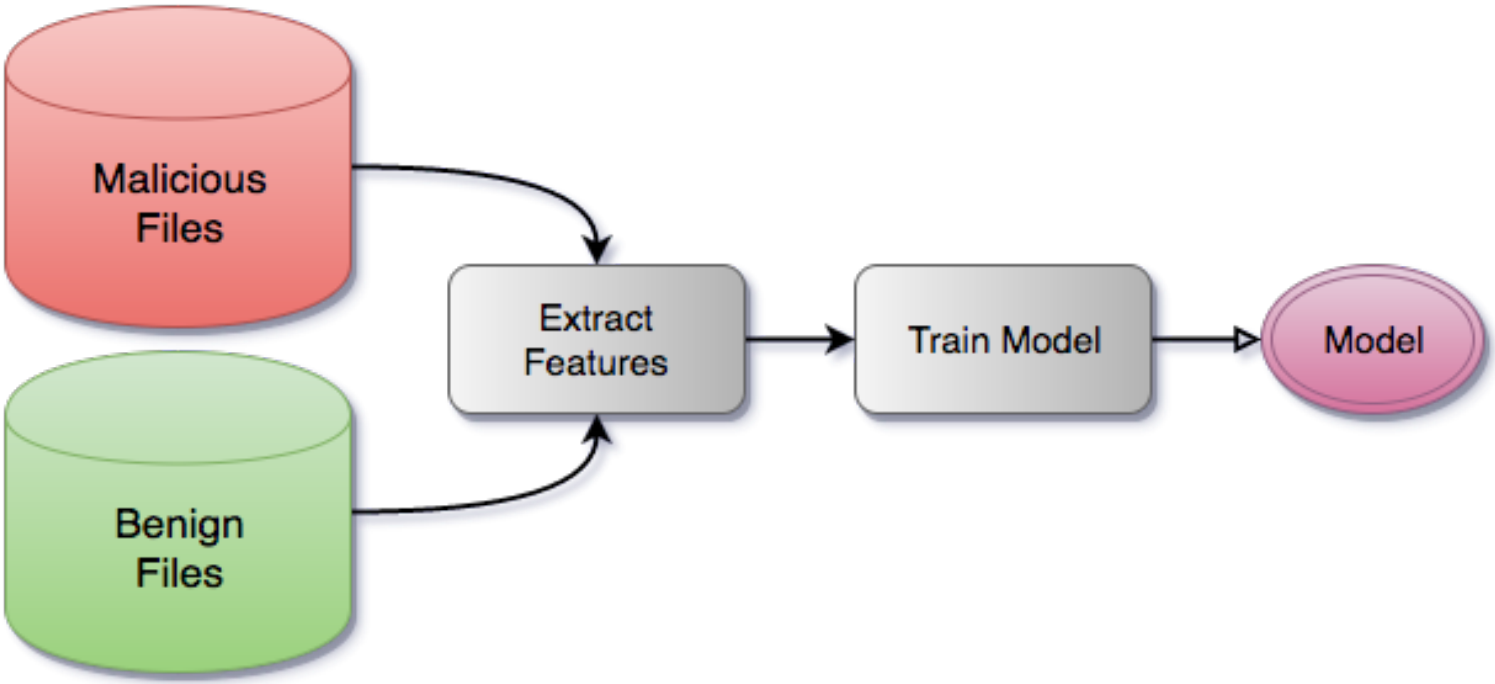


Hình: ibm.com

Demo

Tạo một chương trình phát hiện malware sử dụng machine learning.

- Input: Một file thực thi
- Ouput: File thực thi có phải là malware hay không?



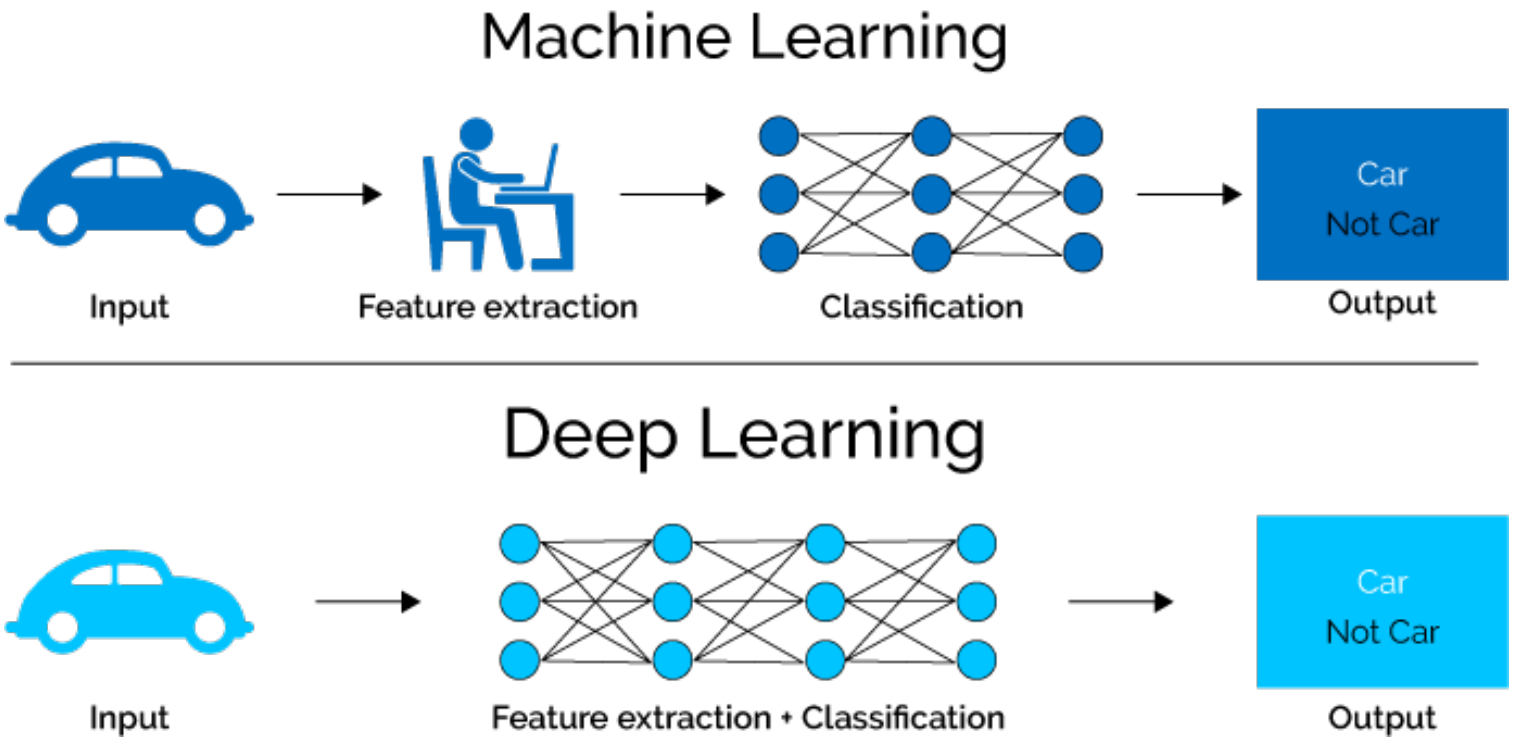
Hình: visionar.today

Implementations

Gần 100 dòng code python.

- Dataset: 185 malware và 195 benign.
- Features: Kích thước file và số lượng sections
- Thư viện: pefile, numpy, scikitlearn.

Deep learning vs Machine learning



Hình: xenonstack.com

Ứng dụng

Hình: slideshare.net

Machine learning then continues to add to its teaching set. Every photo that it identifies — correctly or incorrectly — gets added to the teaching set, and the program effectively gets "smarter" and better at completing its task over time.

It is, in effect, learning.

1. **Data Security**

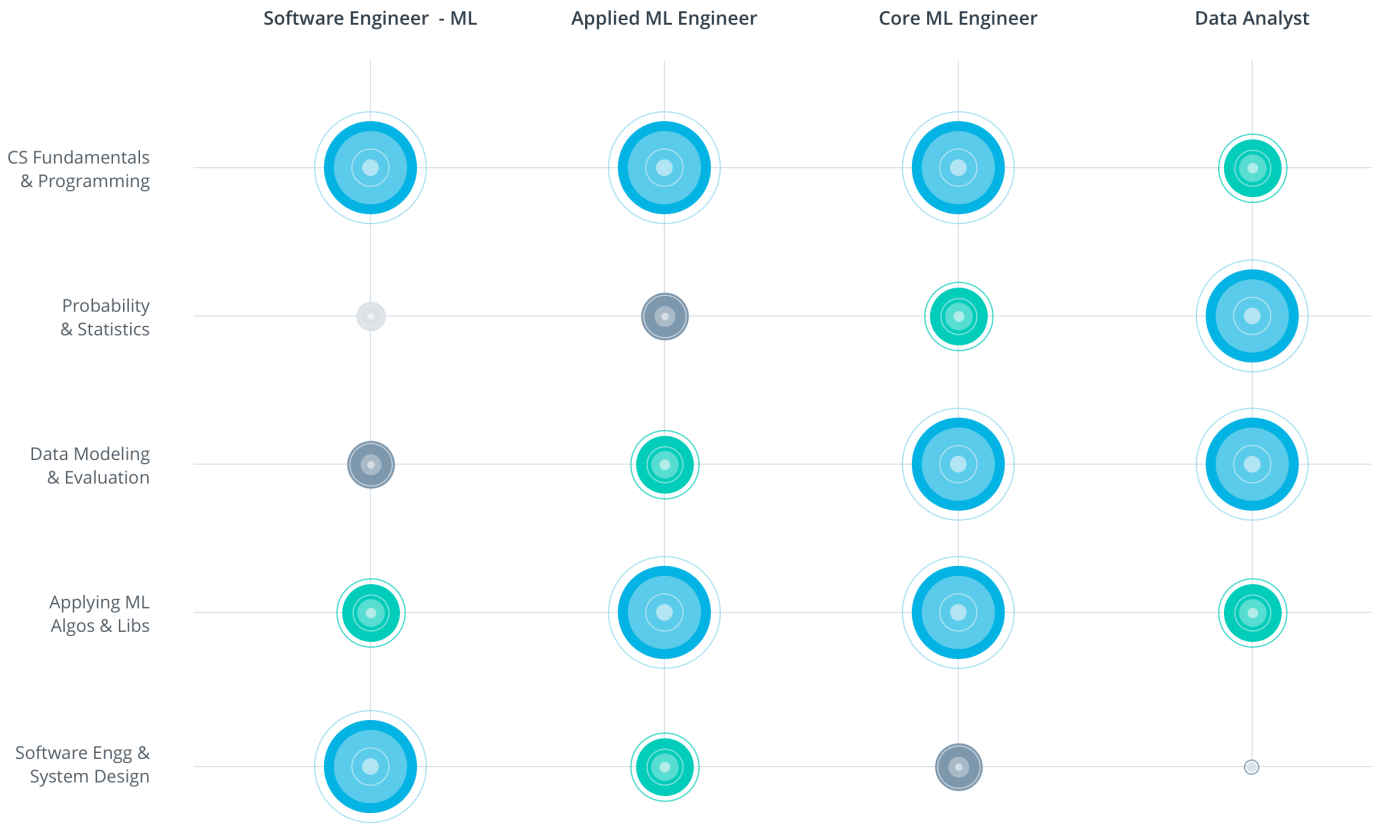
   Malware is a huge — and growing — problem. In 2014, Kaspersky Lab said it had detected 325,000 new malware files *every day*. But, institutional intelligence company Deep Instinct says that each piece of new malware tends to have almost the same code as previous versions — only between 2 and 10% of the files change from iteration to iteration. Their learning model has no problem with the 2–10% variations, and can predict which files are malware with great accuracy. In other situations, machine learning algorithms can look for patterns in how data in the cloud is accessed, and report anomalies that could predict security breaches.

Hình: forbes.com

Ứng dụng

- Phát hiện malware
- Phân loại malware

Kỹ năng



Hình: udacity.com

Cơ hội nghề nghiệp

Hình: kdnuggets.com

The End