NT522 – Phương pháp học máy trong an toàn thông tin

BEE SECURE

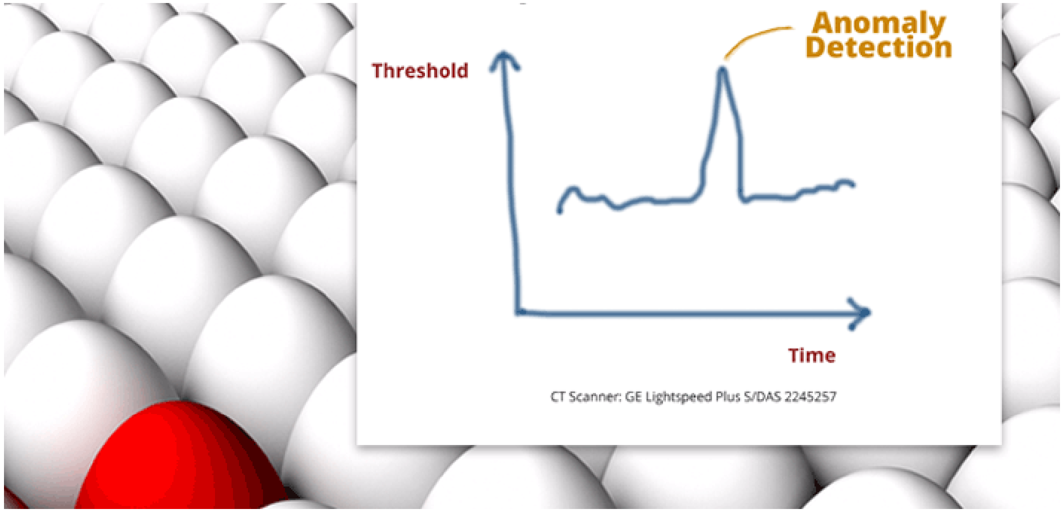
INSECLAB

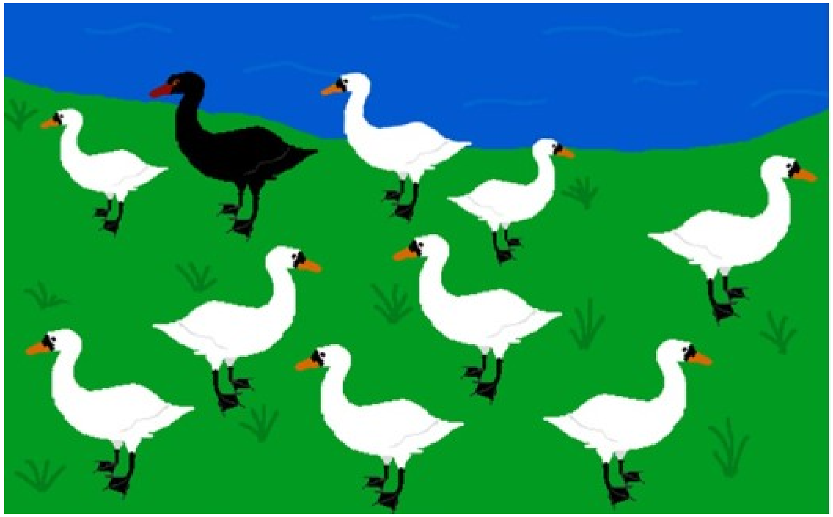
NT522 - Machine Learning for Cybersecurity

UIT InSecLab

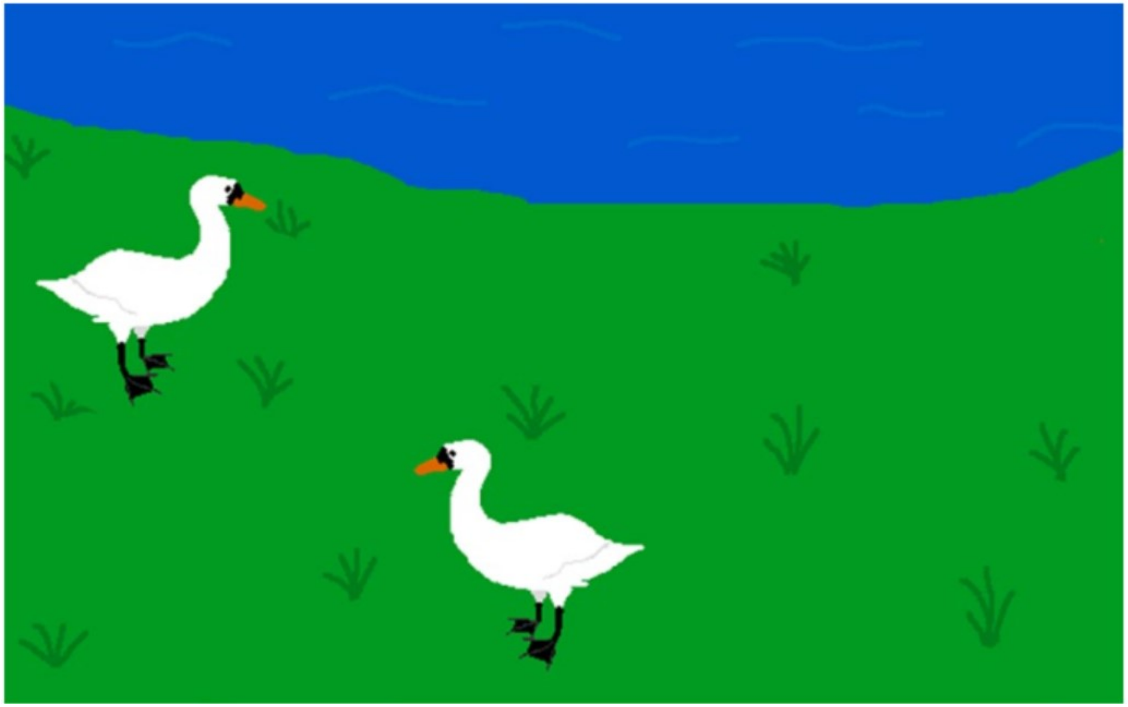
Email: inseclab@uit.edu.vn

Anomaly Detection



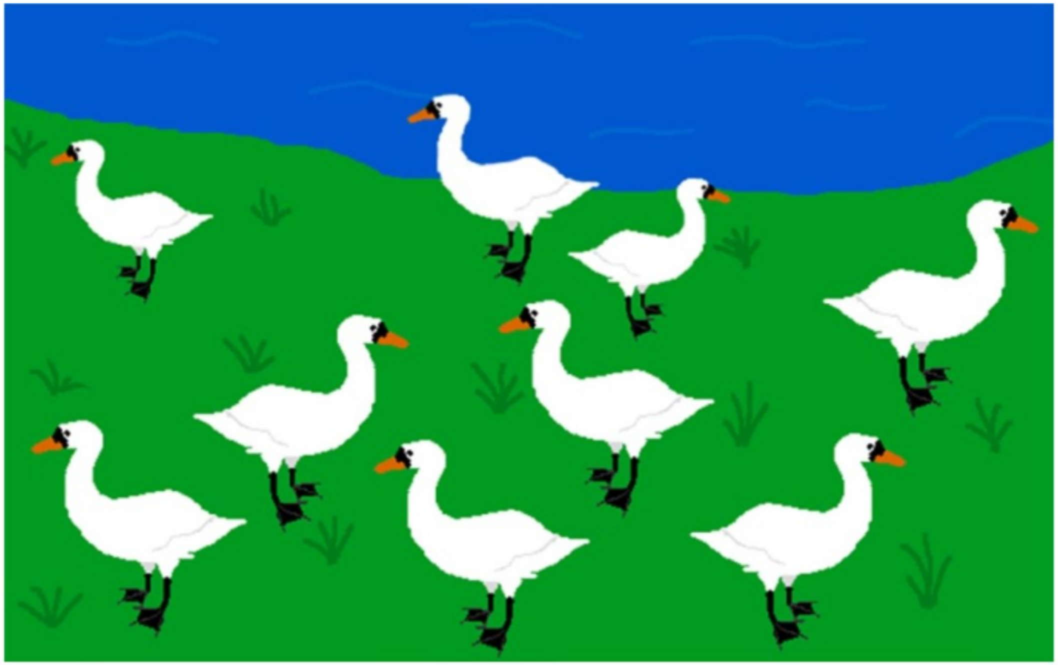


What’s an Anomaly



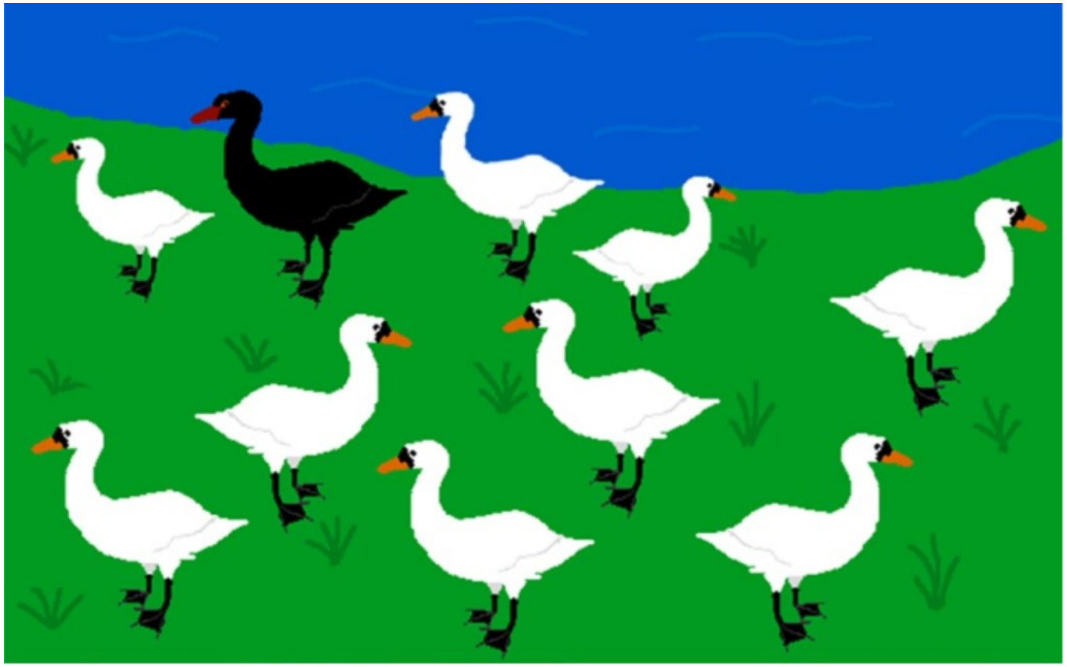
- Observe these swans and make assumptions about the color of the swans.
- Your goal is to determine the normal color of swans and to see if there are any swans that are of a different color than this.

What’s an Anomaly



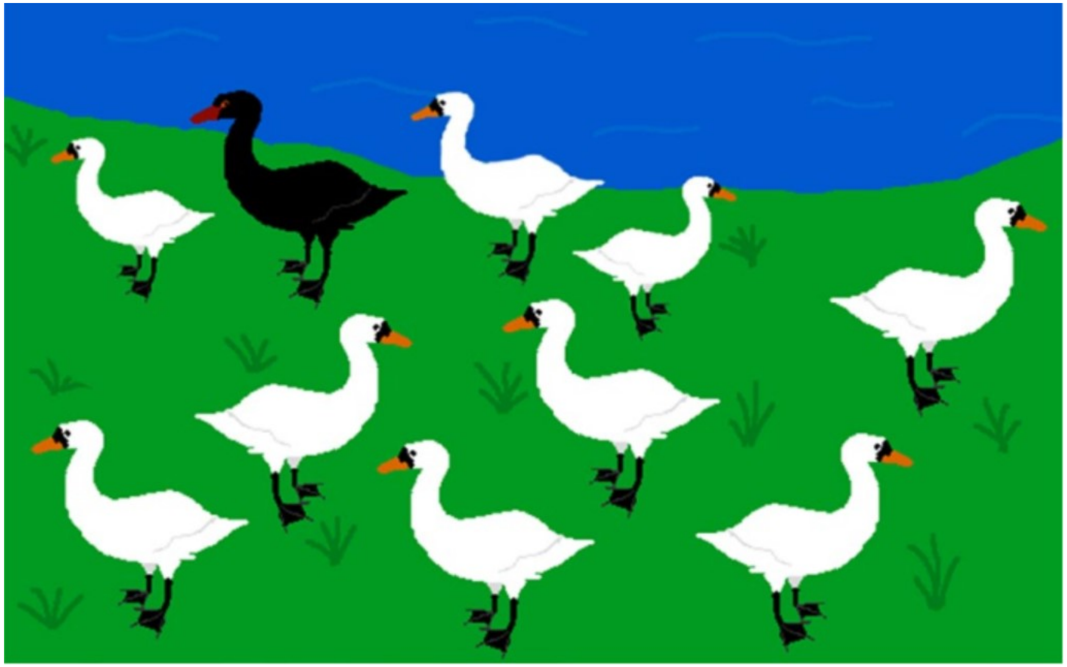
- More swans show up, and they’re all white swans
- It seems reasonable to assume that all swans at this lake are white

What’s an Anomaly



- A black swan appears…
- Considering all of your previous observations, you’ve seen enough of the swans to assume that the next swan would also be white. However, the black swan you see defies that entirely, making it an anomaly.

What’s an Anomaly

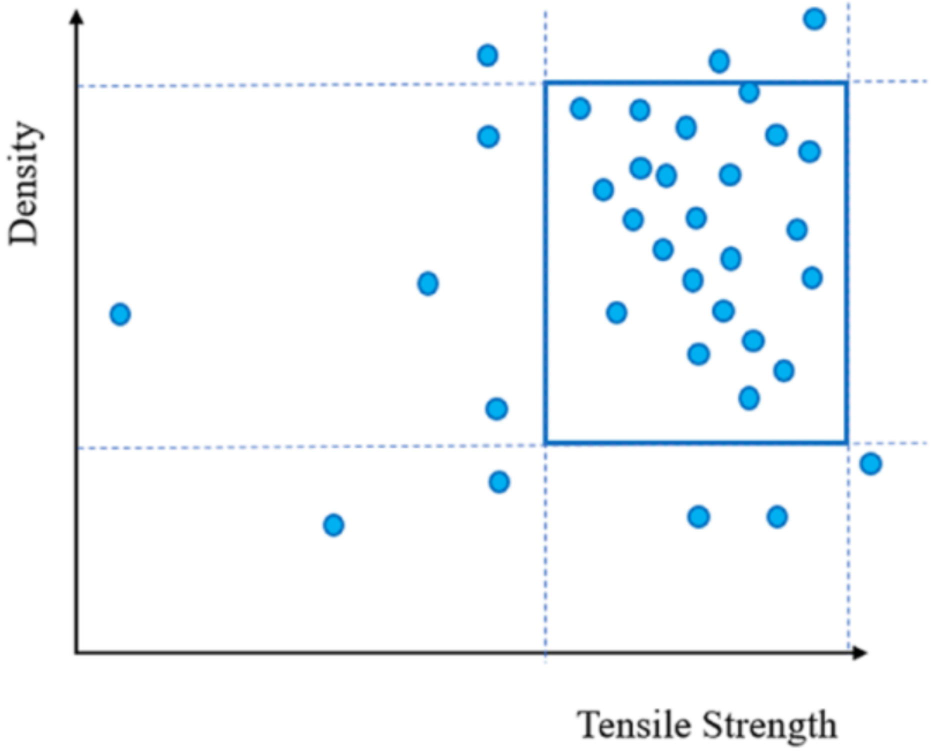


- Given that a vast majority of swans observed at this particular lake are white, you can assume that the normal color for a swan here is white.
- Given a swan by the lake, the probability of it being black is very small. You will consider it an anomaly because of its extreme rarity at this lake

What’s an Anomaly

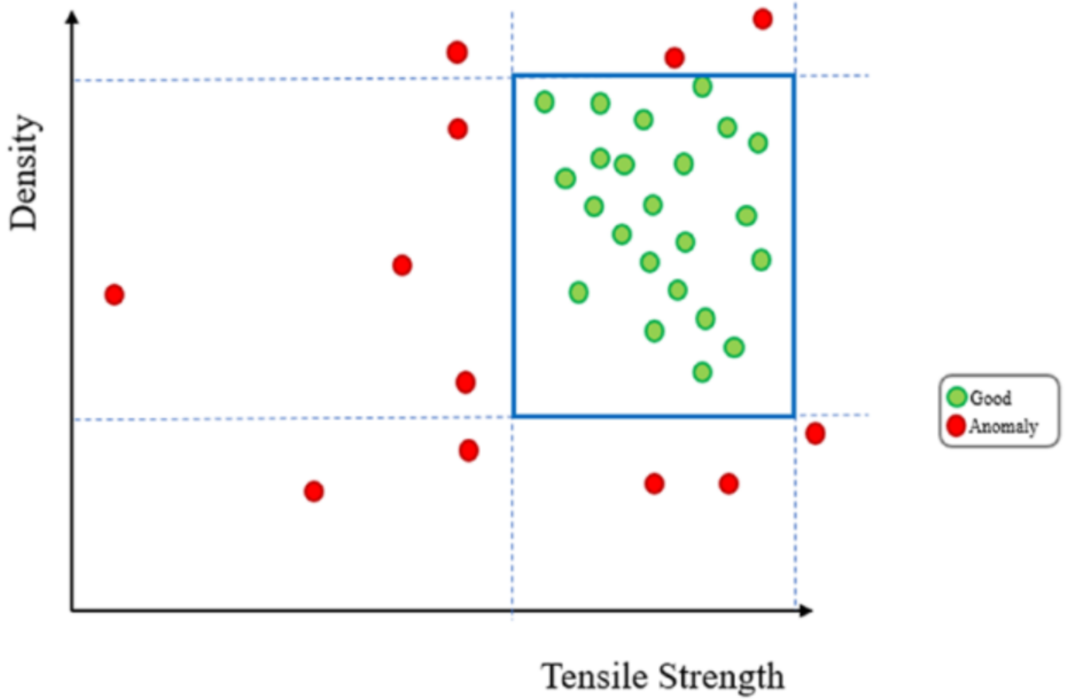
An **anomaly** is an ***outcome*** **or** **value** that deviates from what is expected, but the exact criteria for ***what determines an anomaly*** can ***vary from situation to situation***.

Anomalies as Data Points



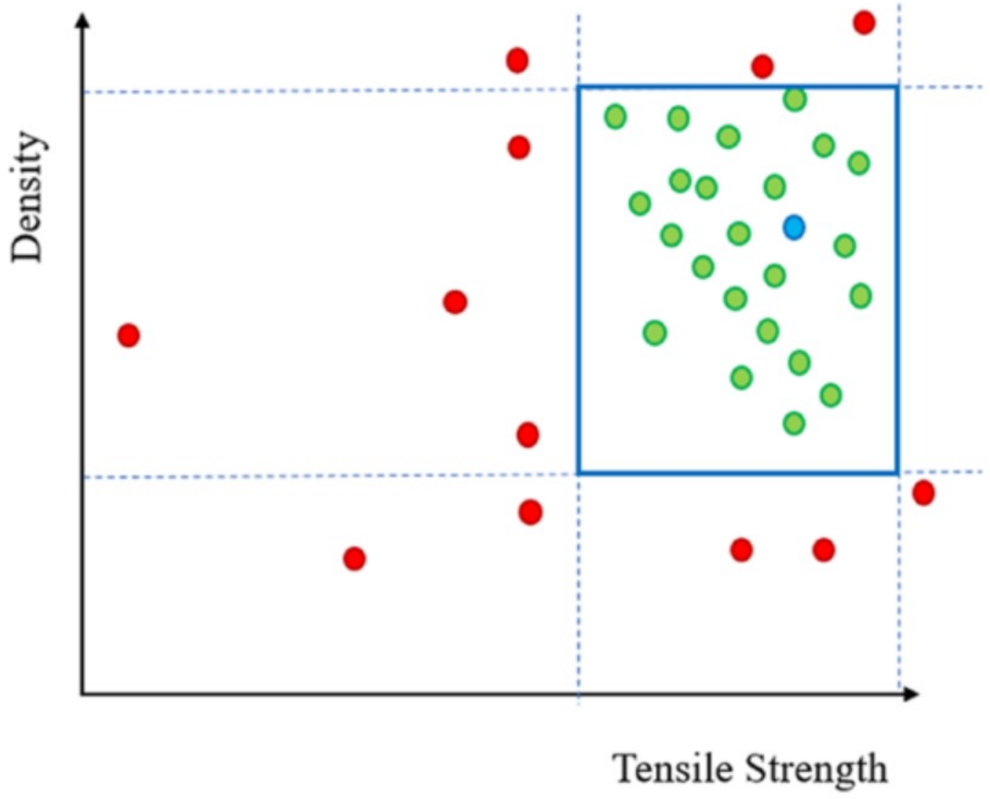
- *Density and tensile strength in sample batches of screws*

Anomalies as Data Points



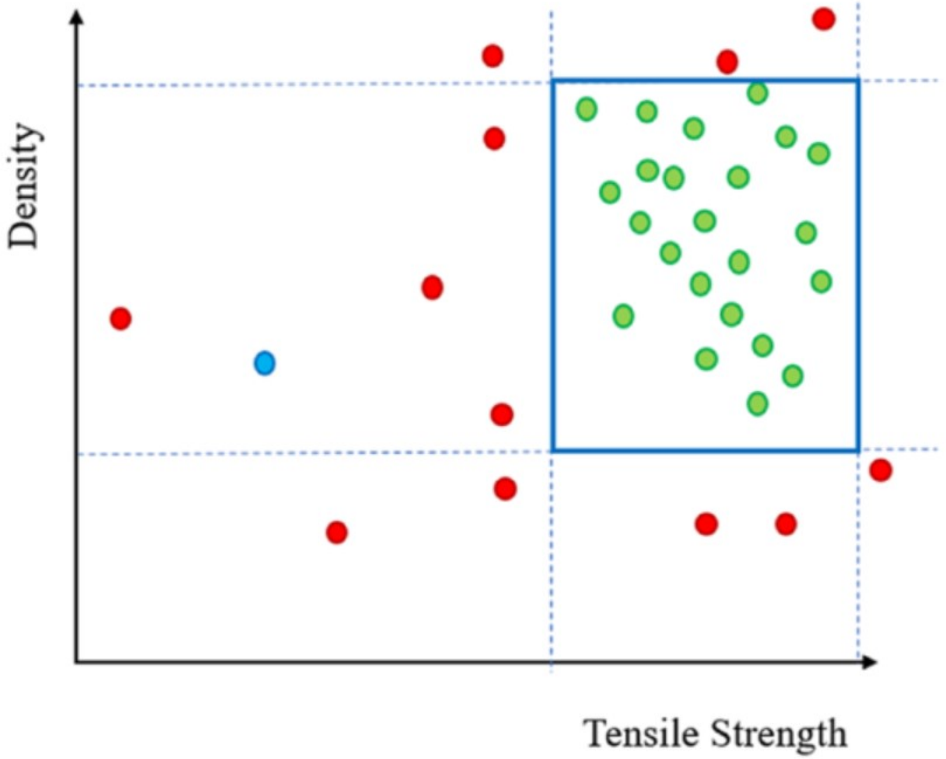
- *Data points are identified as good or anomaly based on their location*

Anomalies as Data Points



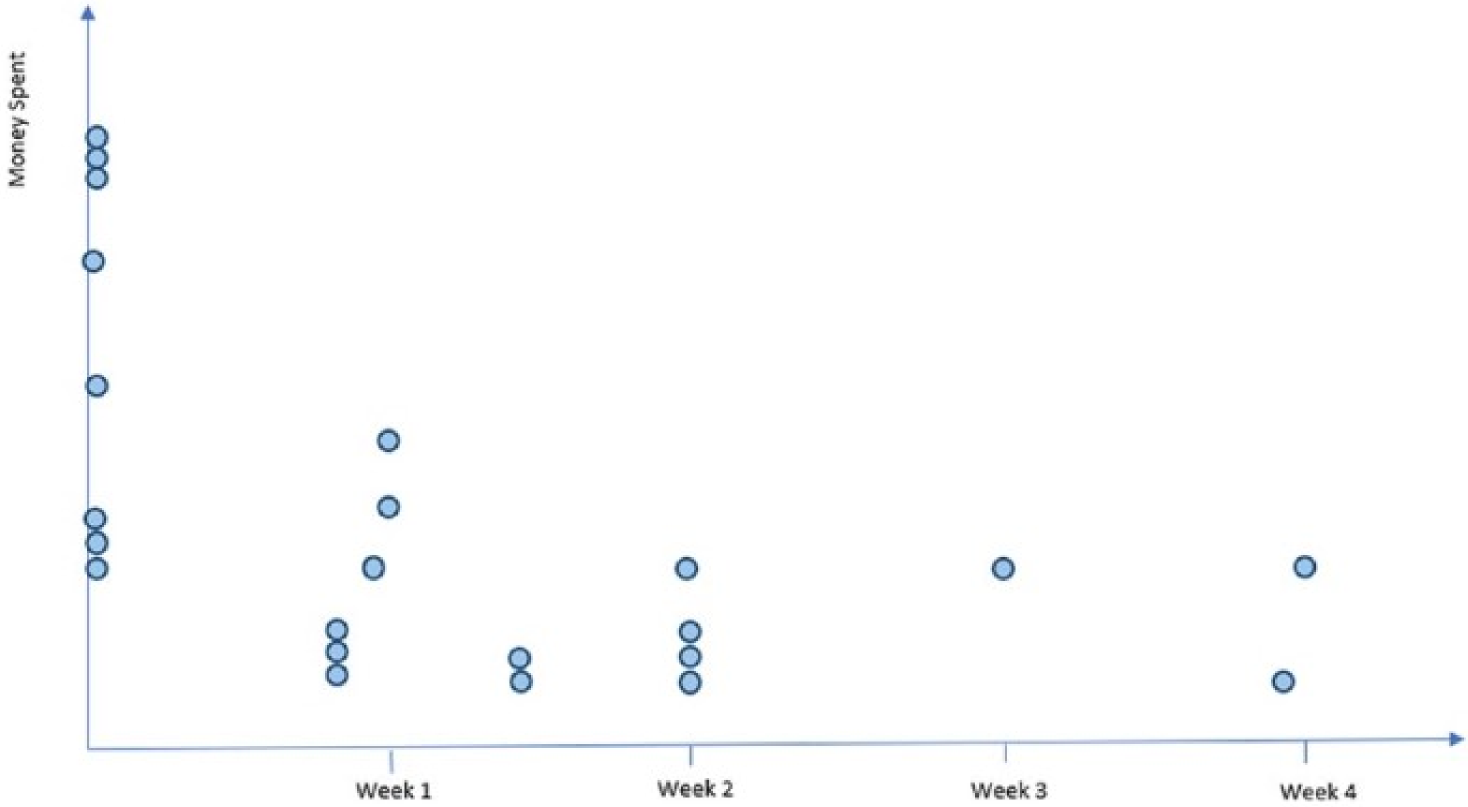
A new data point representing the new sample screw is generated, with the data falling within the bounding box

Anomalies as Data Points



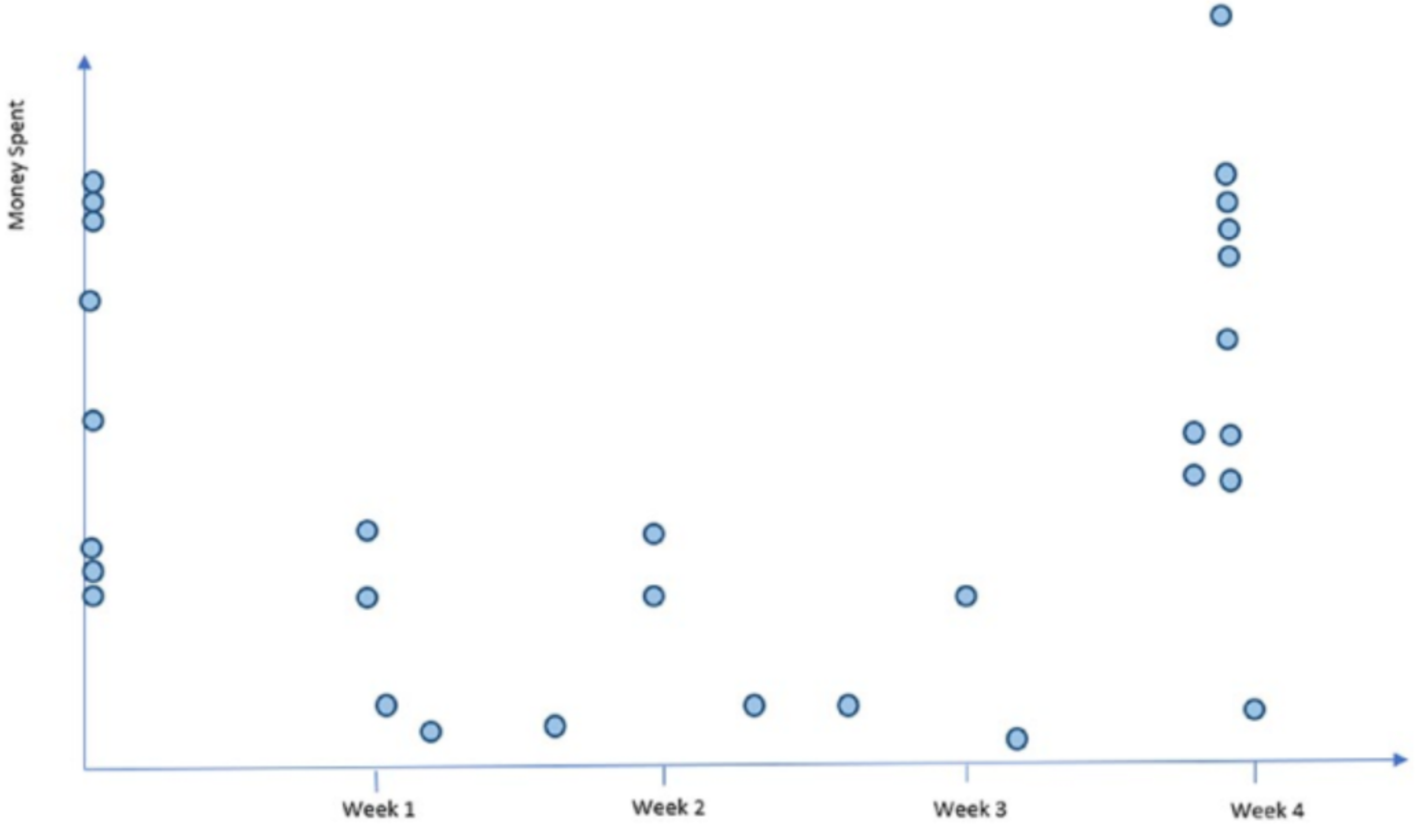
A new data point is generated for another sample, but it falls outside the bounding box

Anomalies in a Time Series



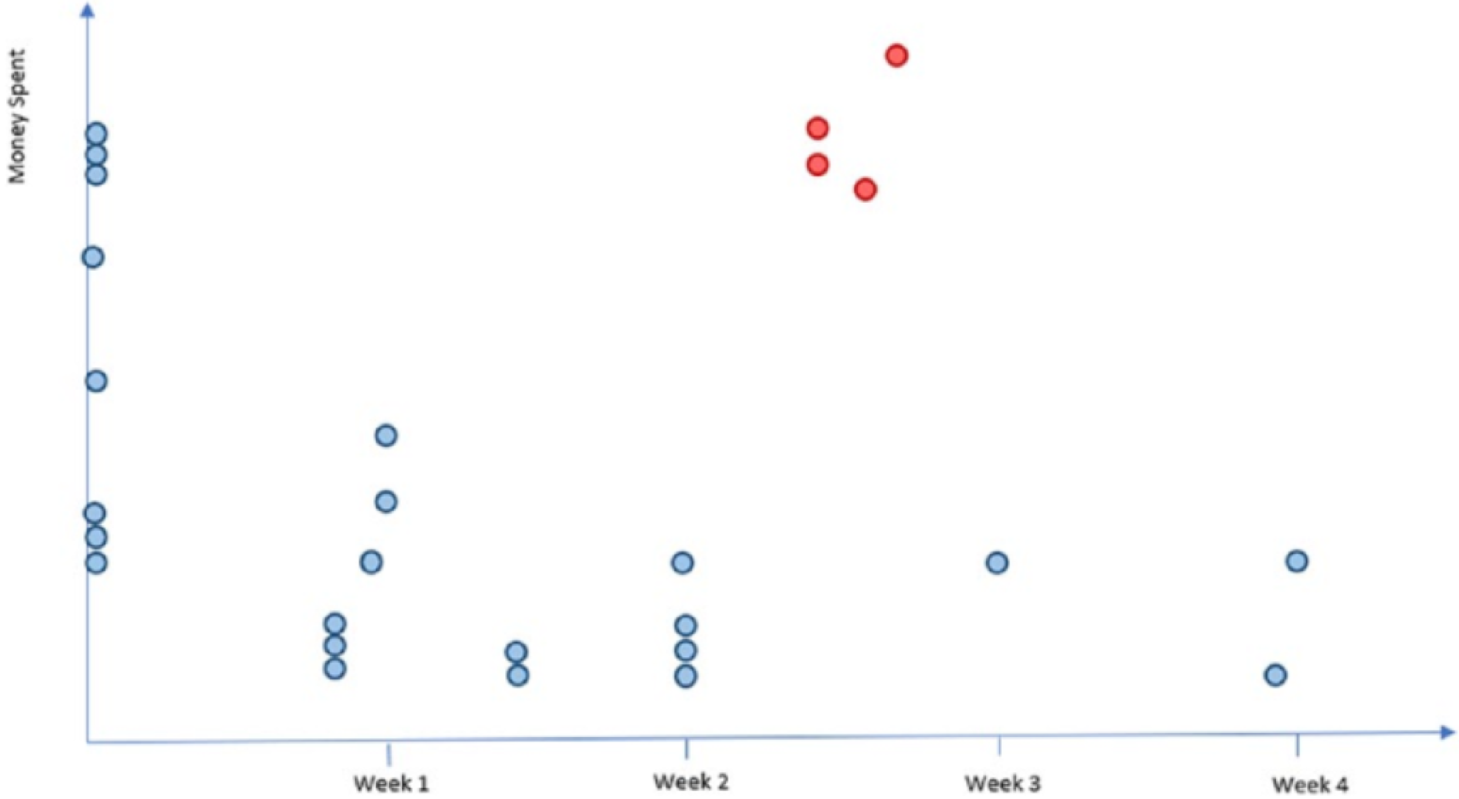
(A) Spending habits of a person over the course of a month

Anomalies in a Time Series



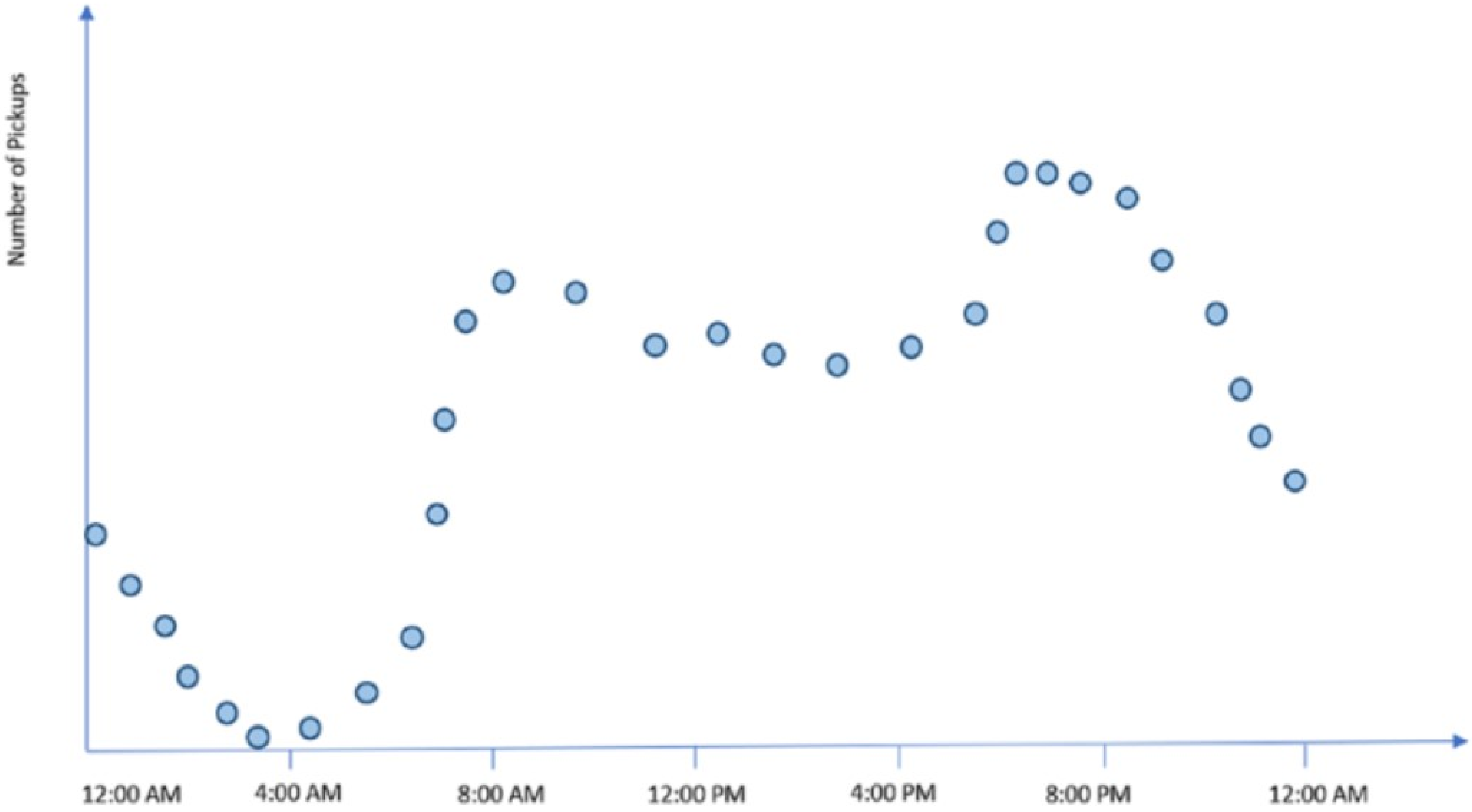
(B) Spending habits for the same person during the month of November (Black Friday)

Anomalies in a Time Series



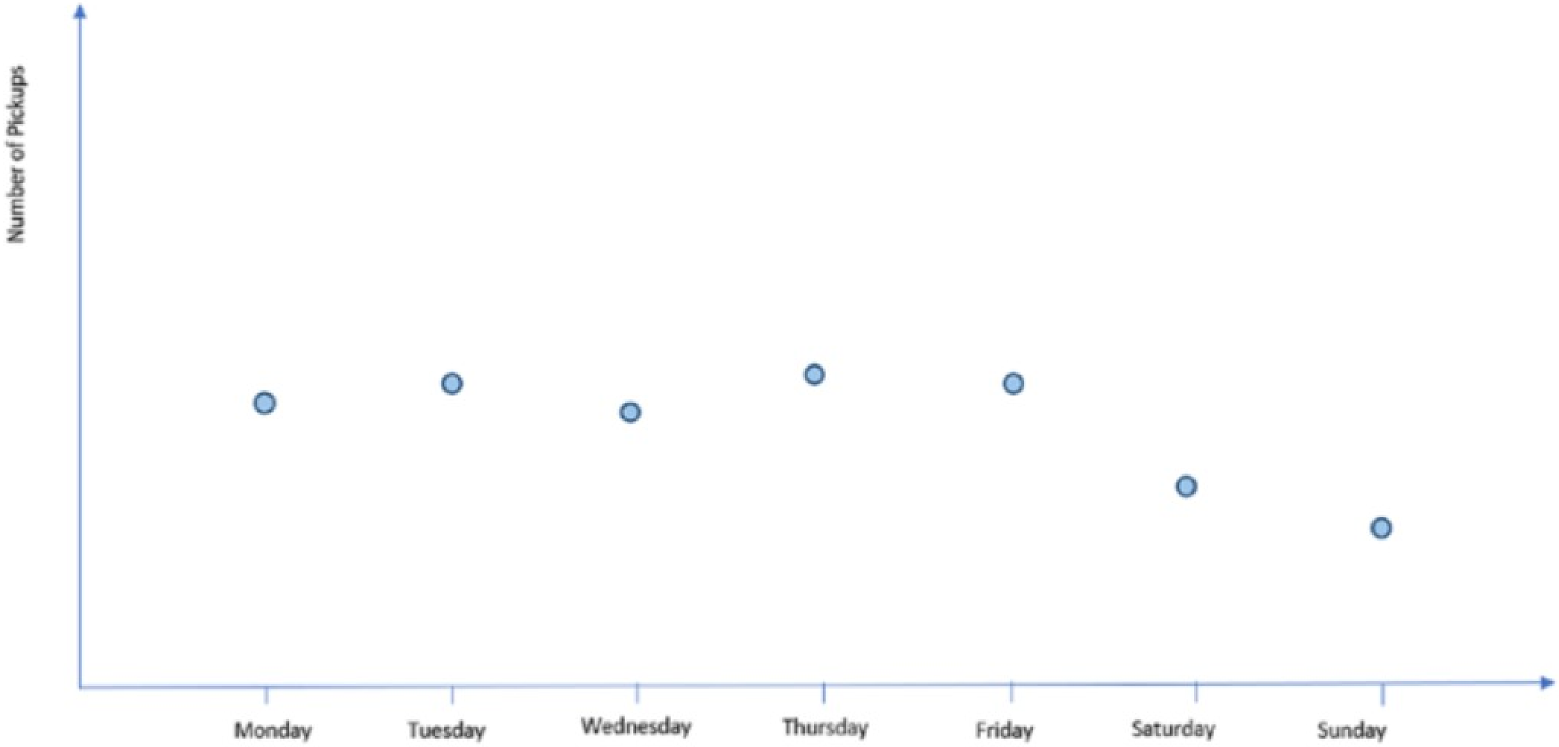
(c) Graph of purchases for the person during the same month as (A), but with credit card stolen

Taxi Cabs



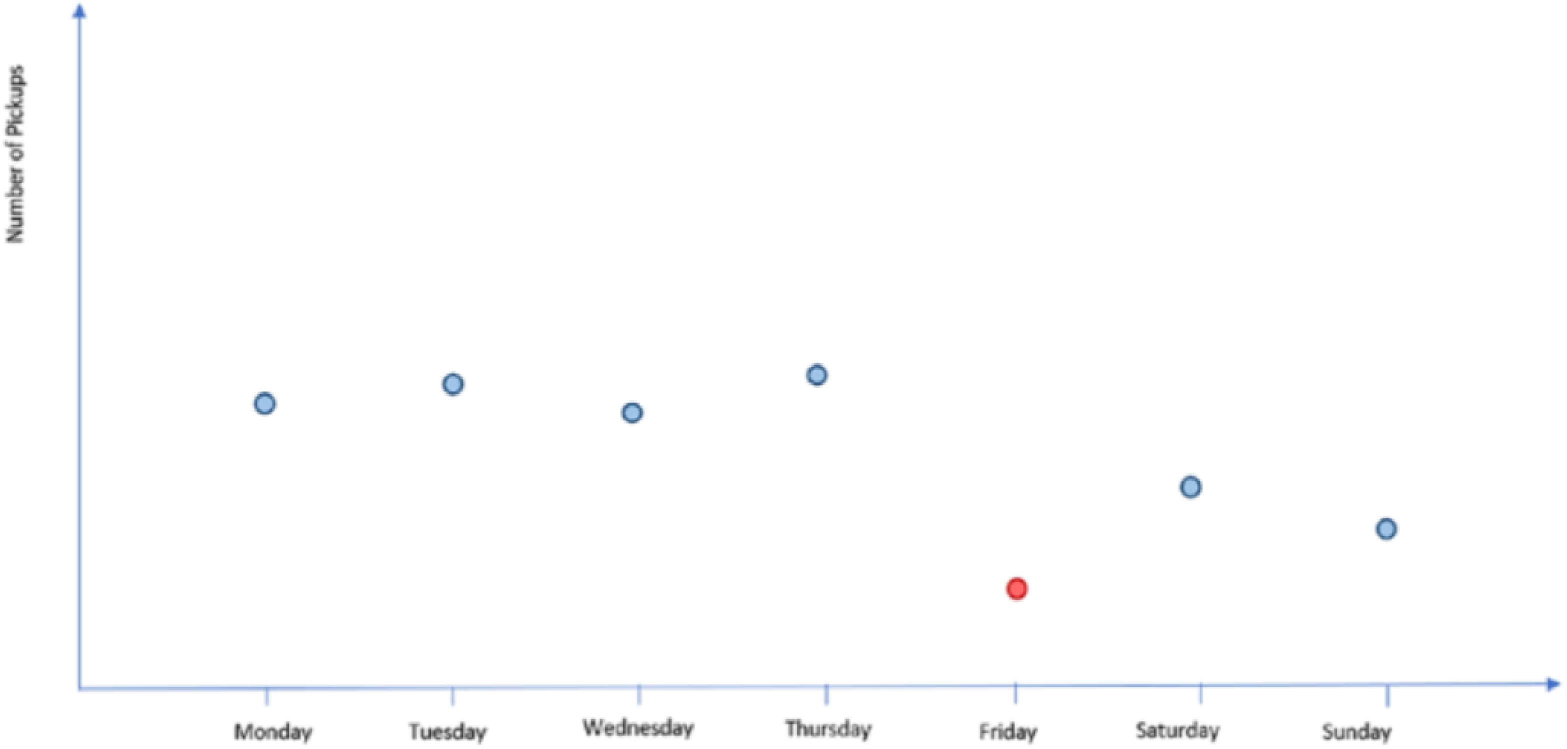
Graph of the number of pickups for a taxi company throughout the day

Taxi Cabs



Graph of the number of pickups for a taxi company throughout the week

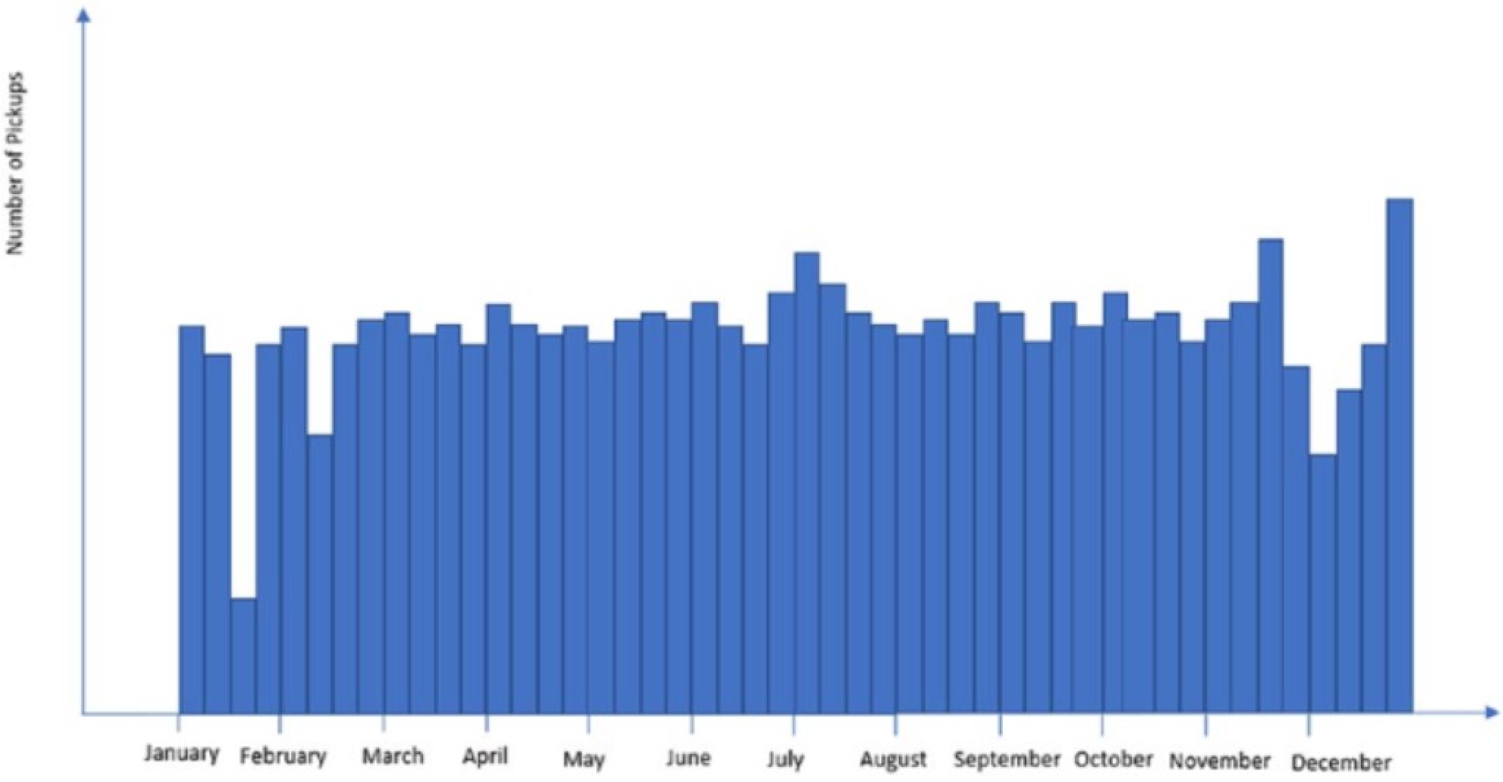
Taxi Cabs



Graph of the number of pickups for a taxi company throughout the week, with a heavy thunderstorm on Friday.

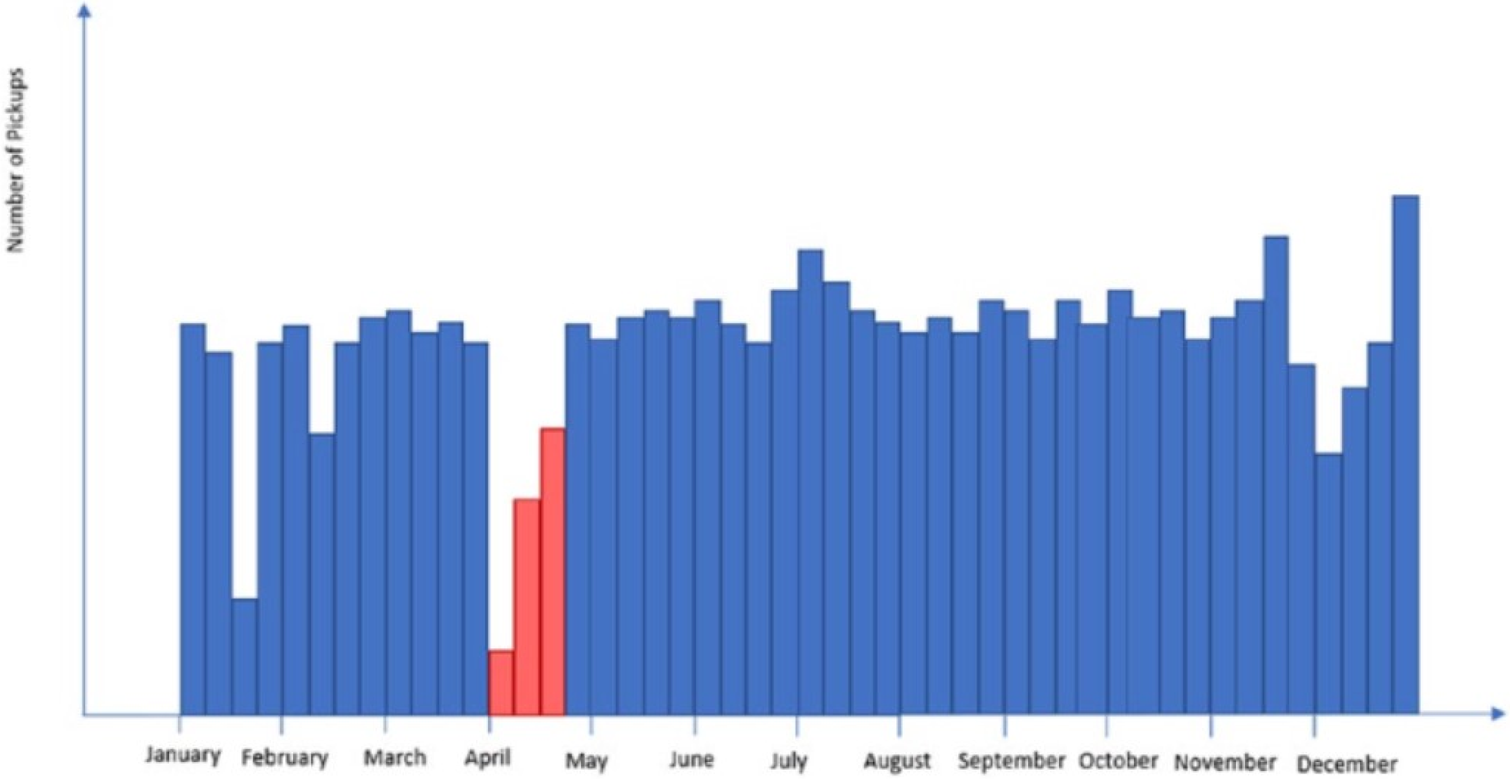
The presence of the thunderstorm could have influenced some people to stay indoors, resulting in a lower number of pickups than usual for a weekday

Taxi Cabs



Number of pickups for a taxi company throughout the year

Taxi Cabs



Number of pickups for a taxi company throughout the year, with a polar vortex hitting the city in April → Pattern rare for the month of April.

Categories of Anomalies

- Data point-based anomalies
- Context-based anomaly
- Pattern-based anomaly

Anomaly Detection

Anomaly detection is the process in which an advanced algorithm **identifies certain data** or **data patterns** to be anomalous. There are 3 tasks of:

- Outlier Detection
- Noise Removal
- Novelty Detection

Outlier Detection

Outlier detection is a technique that aims to detect anomalous outliers within a given data set.

Three ways can be applied in this situation:

- Train only on normal data to identify anomalies by a high reconstruction error.
- Model a probability distribution in which anomalies are labeled based on their association with really low probabilities
- Train a model to recognize anomalies by teaching it what an anomaly looks like and what a normal point looks like

Noise Removal

In **noise removal**, there is constant background noise in the data set that must be filtered out.

- The model learns an efficient way to represent the original data so that it can reconstruct it without the anomalous interference noise.
- This can also be a case where an image has been altered in some form, such as by having perturbations, loss of detail, fog.
- The model learns an accurate representation of the original image and outputs a reconstruction without any of the anomalous elements in the image.

Novelty Detection

- **Novelty detection** is very ***similar*** to ***outlier detection***. In this case, a novelty is a data point outside of the training set, the data set the model was exposed to, that was shown to the model to determine if it is an anomaly or not.
- **The key difference** between **novelty detection** and ***outlier detection*** is that in outlier detection, the job of the model is to determine what is an anomaly within the training data set.
- In **novelty detection**, the model learns what is a normal data point and what isn’t, and tries to classify anomalies in a new data set that it has never seen before.

The Three Styles of Anomaly Detection

- **Supervised anomaly detection:** *is a technique in which the training data has labels for both anomalies and for normal data points.*
- **Semi-supervised anomaly detection:** *involves partially labeling the training data set (ex. AutoEncoder).*
- **Unsupervised anomaly detection:** *involves training the model on unlabeled data. (ex. Isolation forest)*

Where Is Anomaly Detection Used?

- Data breaches
- Identity Theft
- Manufacturing
- Networking
- Cybersecurity
- Finance
- Medicine
- Video Surveillance

Anomaly Detection

- Applicable in a variety of domains:
  - Intrusion detection, fraud detection, fault detection, system health monitoring, event detection in sensor network
- It is often used in pre-processing to remove anomalous data from the dataset
- In supervised ML, removing anomalous data from the dataset often results in a statistically significant increase in accuracy.

Optimal anomaly detection system

A set of objectives for an optimal anomaly detection system:

- Low false positives and false negatives.
- Easy to configure, tune, and maintain.
- Adapts to changing trends in the data
- Works well across datasets of different nature
- Resource-efficient and suitable for real-time application
- Explainable alerts

Traditional Methods of Anomaly Detection

- **Isolation Forest:** An isolation forest is a collection of individual tree structures that recursively partition the data set. In each iteration of the process, a random feature is selected, and the data is split based on a randomly chosen value between the minimum and maximum of the chosen feature.
  - It works well for multidimensional data, and can be used for unsupervised anomaly detection.
- **One-class Support Vector Machine (OC-SVM):** well-suited for **novelty detection** (an example of *semi-supervised anomaly detection*)

Deep Learning Method

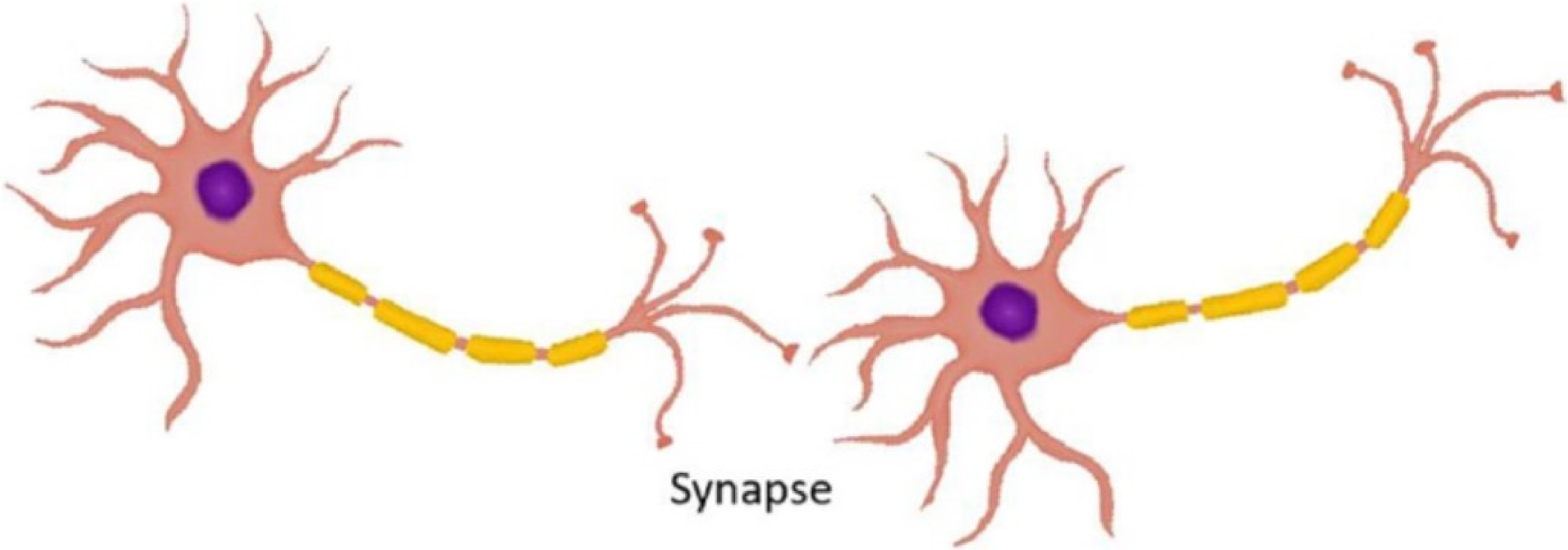
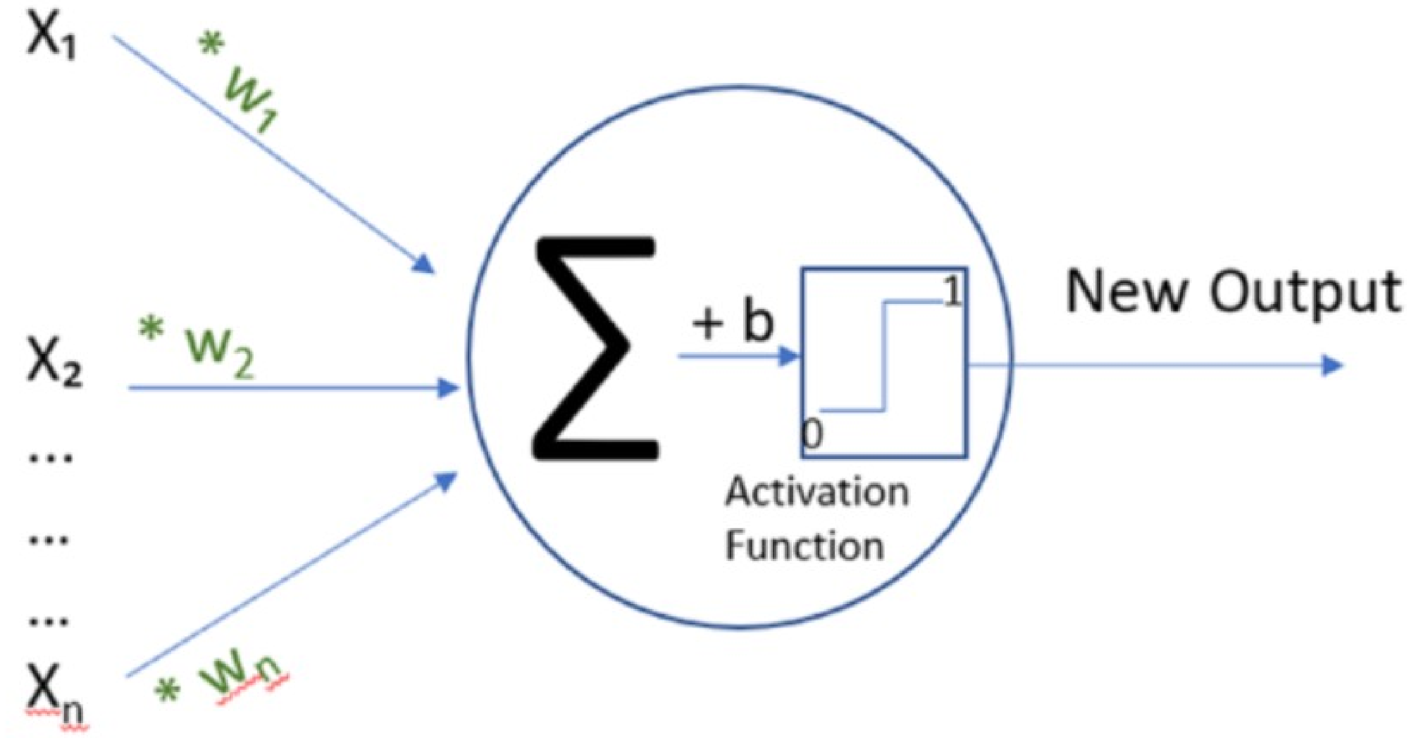
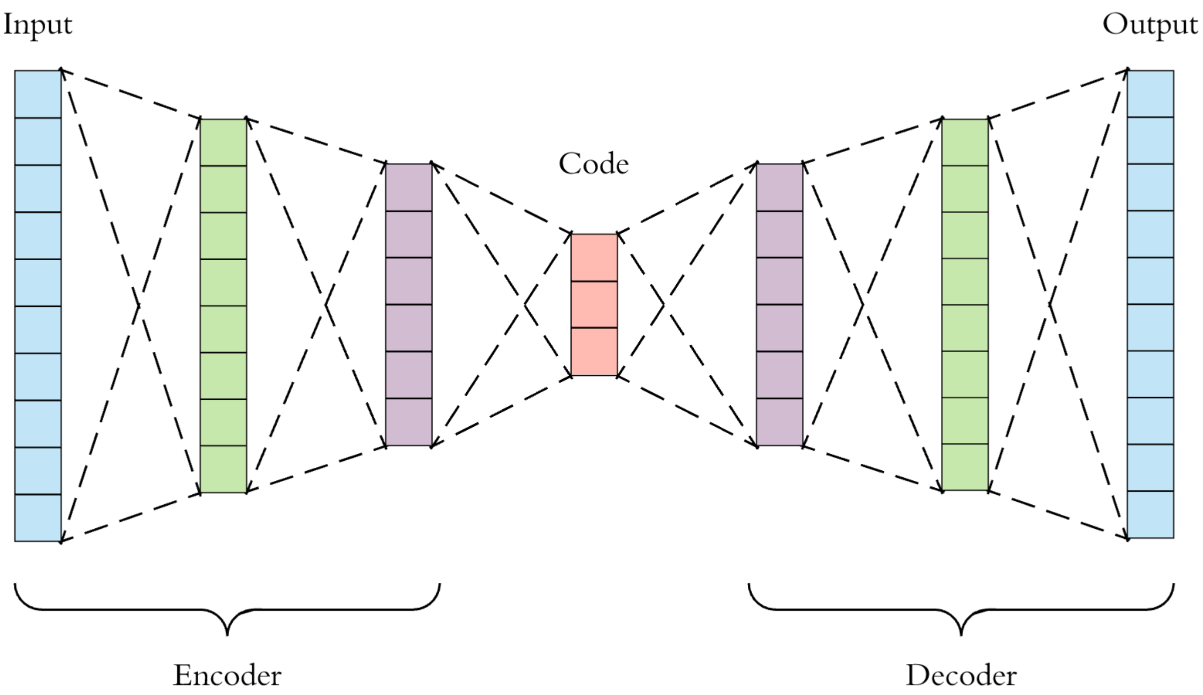


***Figure 3-2.** How two neurons might connect to form a chain and transfer signals through that connection. The terminal axon of the first neuron connects to the dendrites of the second neuron*

Deep Learning Method

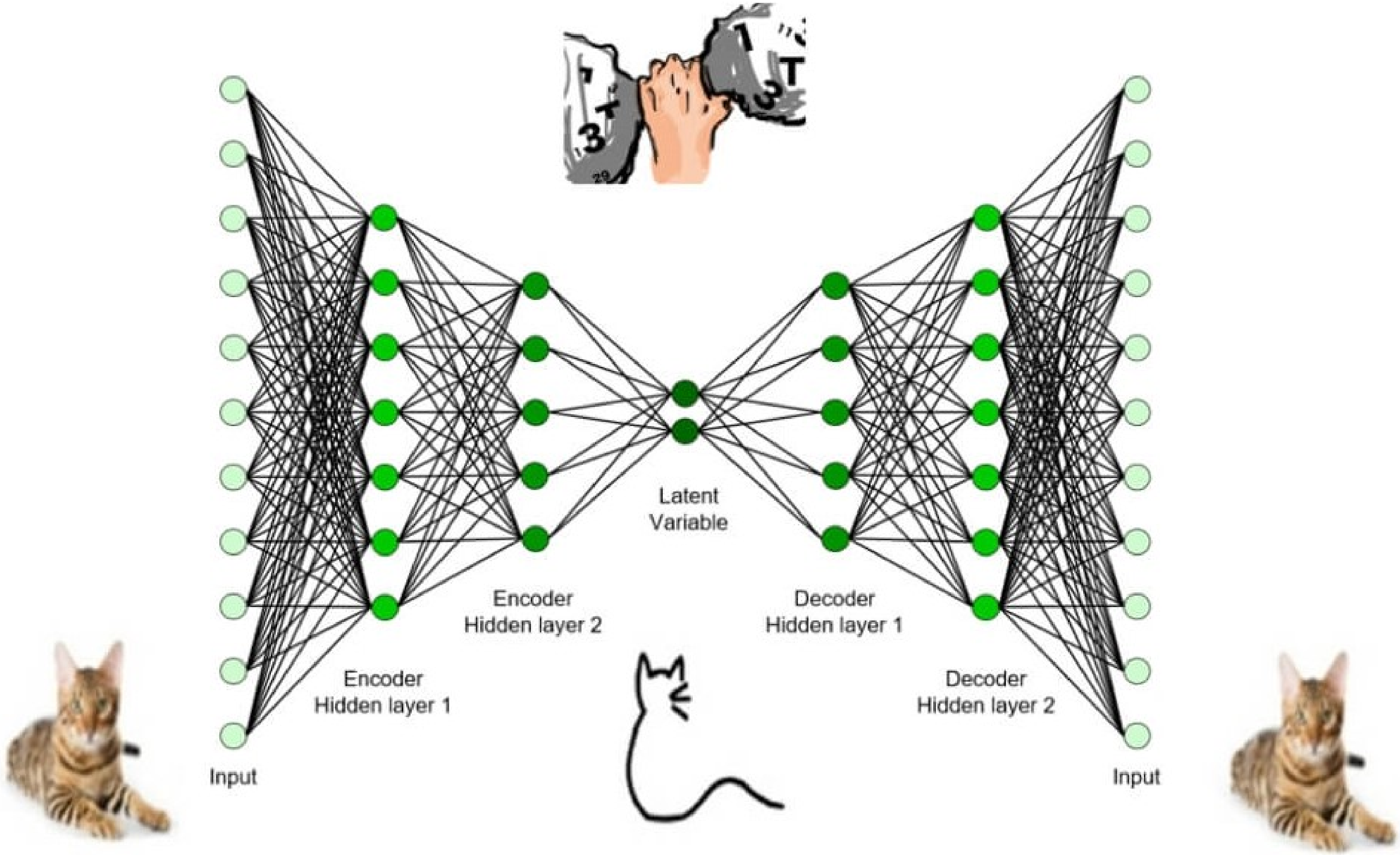


Autoencoders for Anomaly Detection



- Autoencoders are neural networks that have the ability to ***discover low-dimensional representations*** of high-dimensional data and are able to ***reconstruct the input from the output***.
- **Autoencoders** are made up of ***two pieces of the neural network***, an **encoder** and a **decoder**. The encoder reduces the dimensionality of a high dimensional dataset to a low dimensional one whereas a decoder essentially expands the low-dimensional data to high-dimensional data.

Autoencoders for Anomaly Detection



AutoEncoder

Autoencoders for Anomaly Detection

Some popular applications of AutoEncoders are:

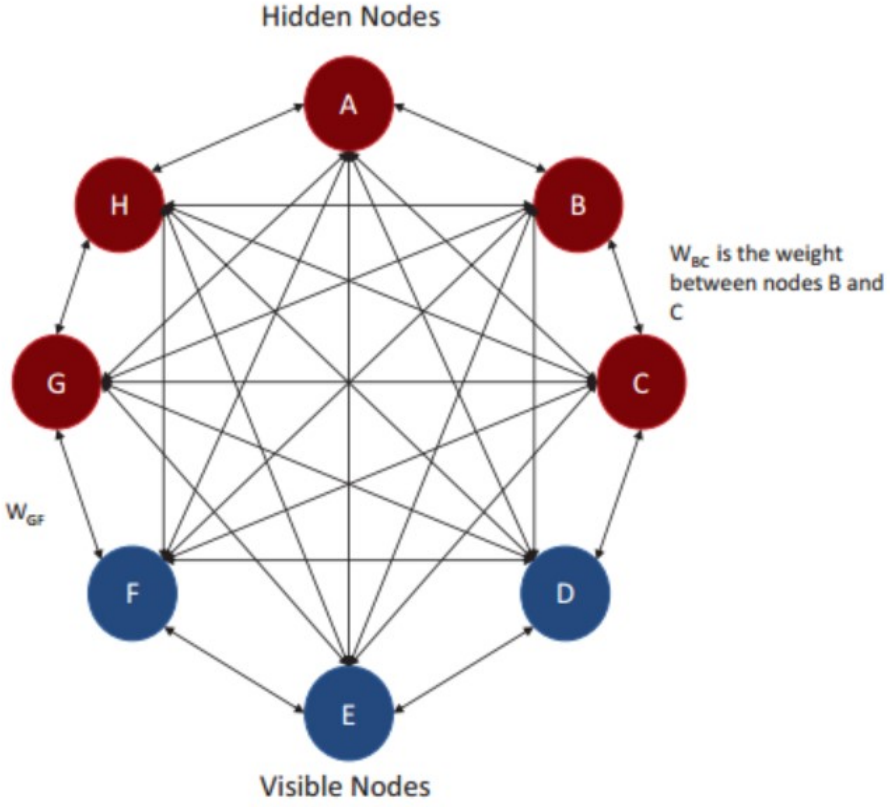
- Training Deep Learning network
- Compression
- Classification
- **Anomaly Detection**
- Generative Models

Autoencoders for Anomaly Detection

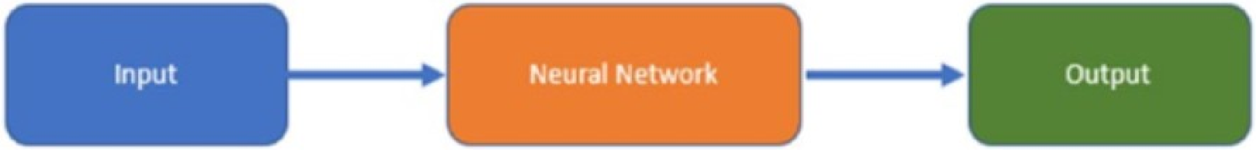
- Simple autoencoders
- Sparse autoencoders
- Deep autoencoders
- Convolutional autoencoders
- Denoising autoencoders
- Variational autoencoders

Boltzmann Machines for Anomaly Detection

- A graph showing how a **Boltzmann machine** can be structured.
- Notice that all of the nodes are interconnected, even if they are in the same layer
- Now, it is replaced with the newer Deep Learning models.

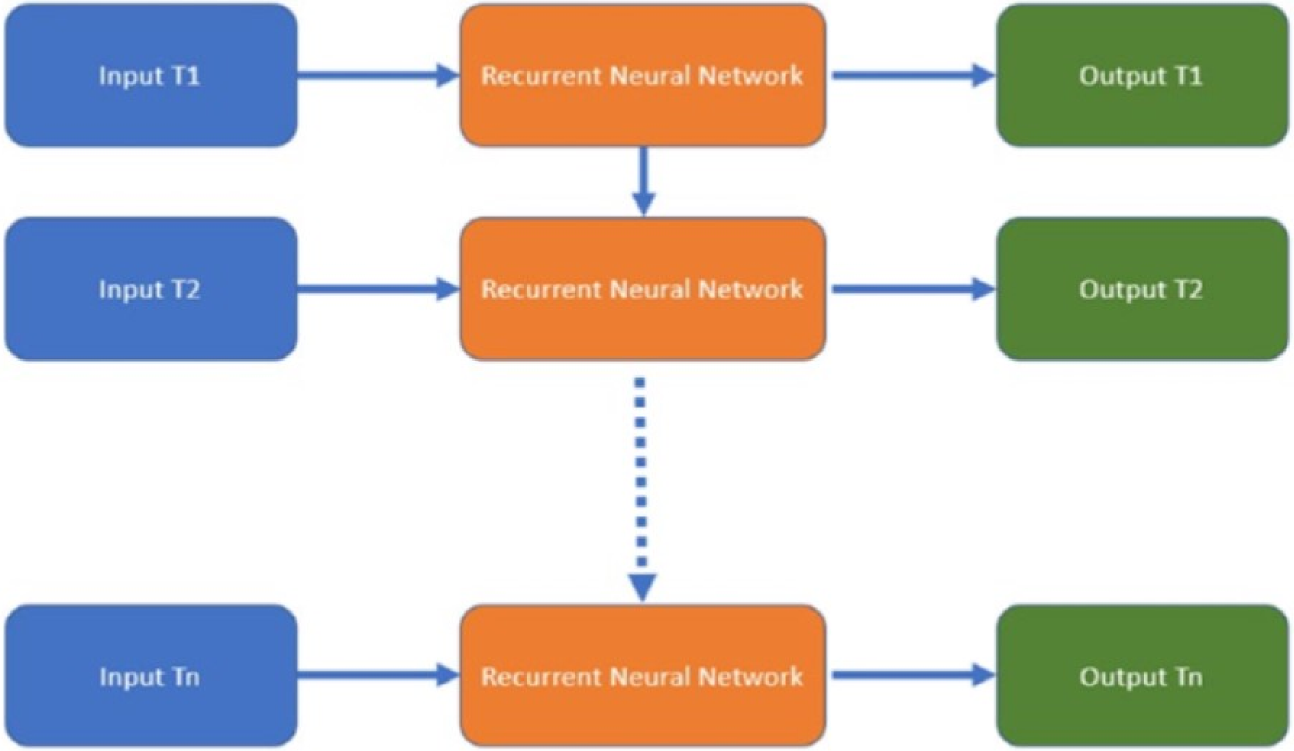


Long Short-Term Memory Models for Anomaly Detection



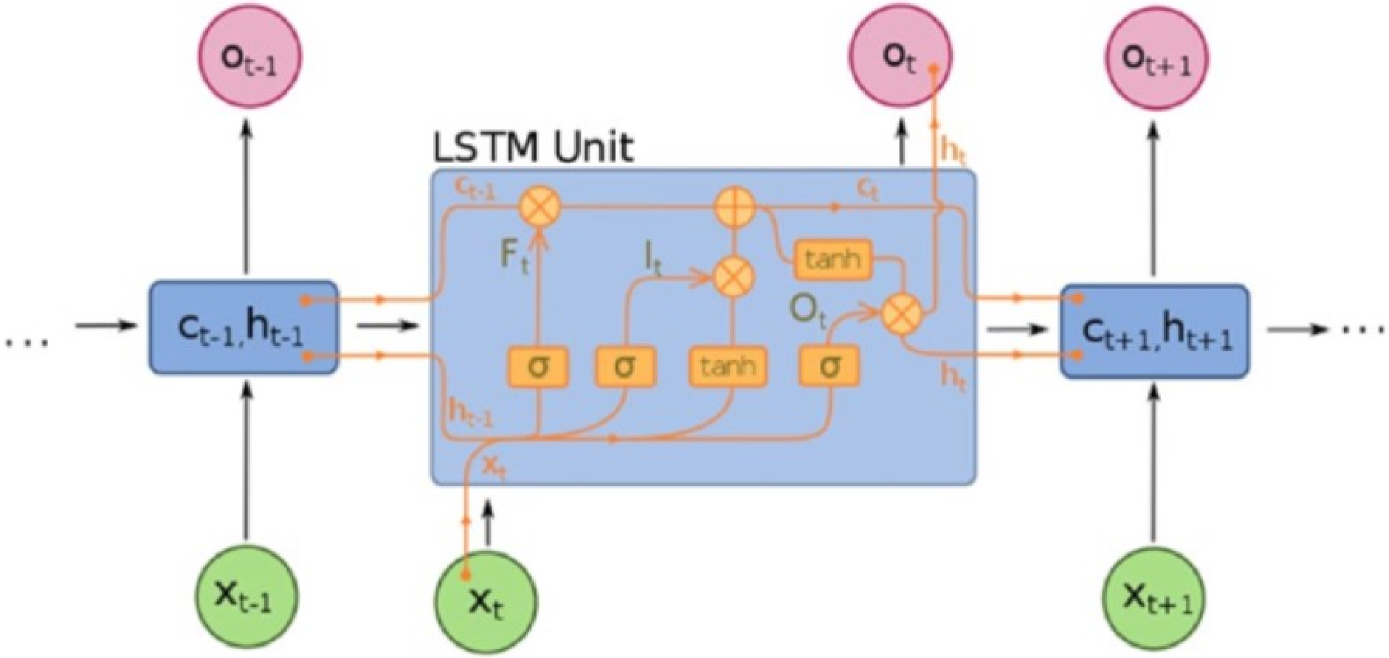
A high-level representation of neural networks

Long Short-Term Memory Models for Anomaly Detection



A recurrent neural network (RNN)

Long Short-Term Memory Models for Anomaly Detection

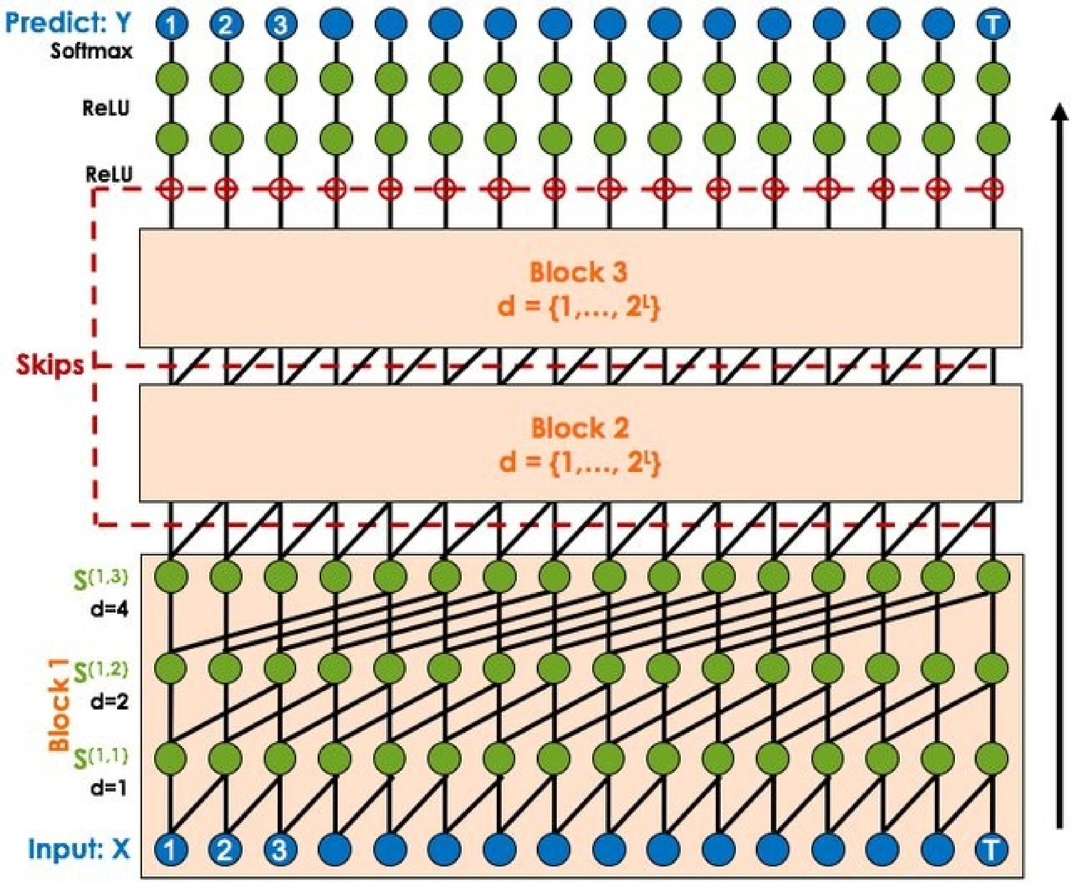


A detailed LSTM network

Temporal Convolutional Network for Anomaly Detection

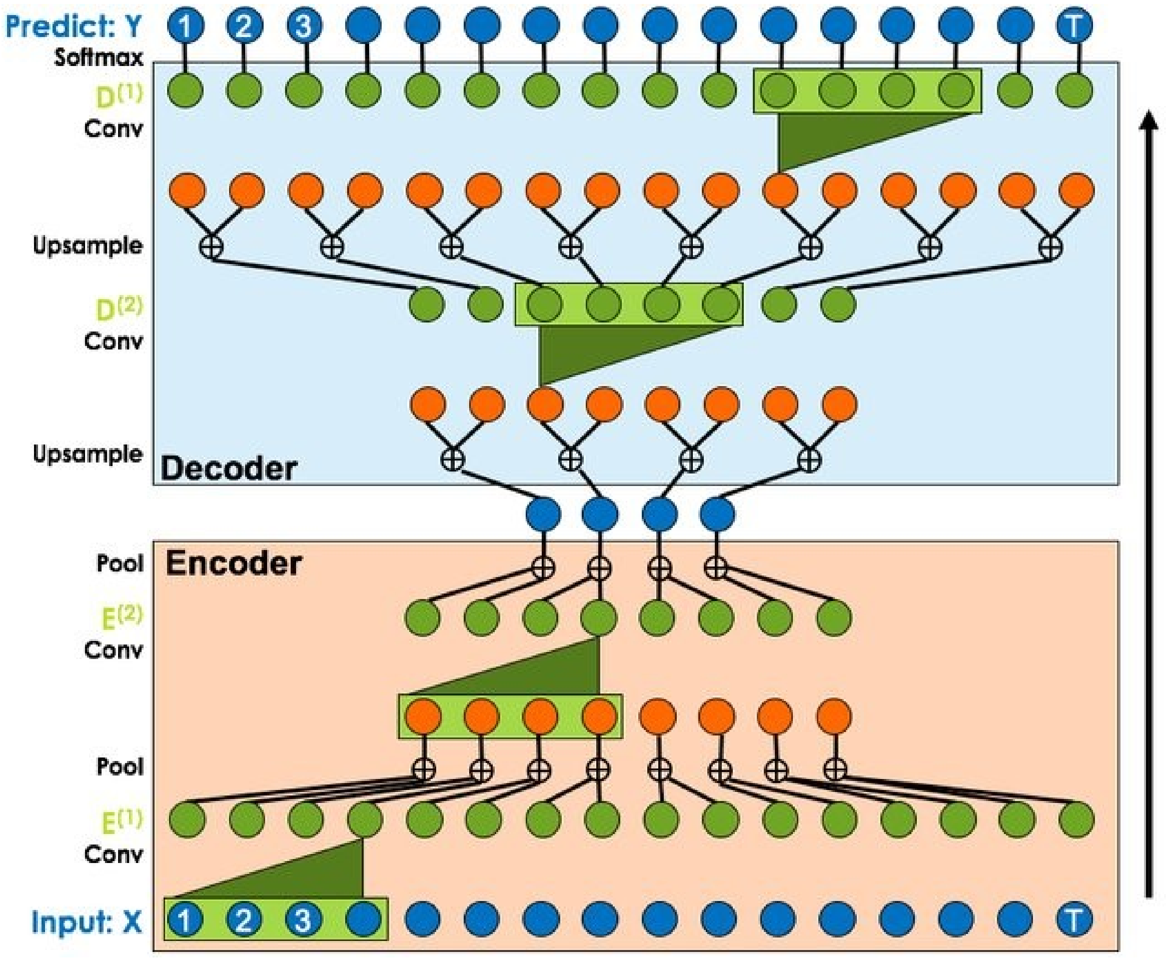
- Dilated Temporal Convolutional Network
- Encoder-Decoder Temporal Convolutional Network

Temporal Convolutional Network for Anomaly Detection



Dilated Temporal Convolutional Network (Dilated TCN)

Temporal Convolutional Network for Anomaly Detection

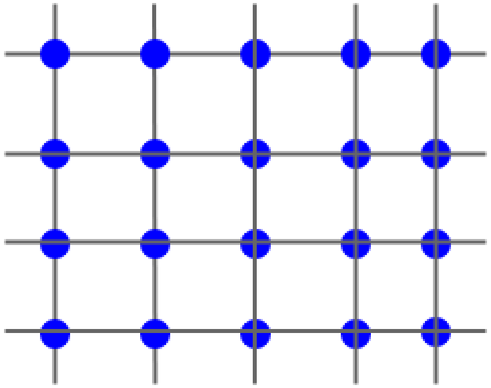


Encoder-Decoder Temporal Convolutional Network (ED-TCN)

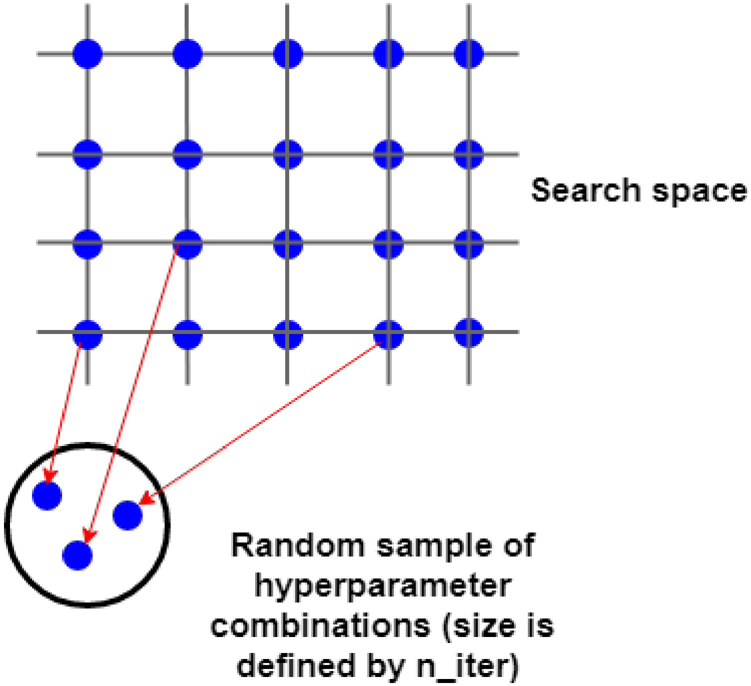
Tips for today: Hyperparameter Optimization

Sikit-learn — the Python machine learning library provides two special functions for hyperparameter optimization:

- **GridSearchCV —** for Grid Search
- **RandomizedSearchCV —** for Random Search



Grid Search


Search space
Random sample of hyperparameter combinations (size is defined by n_iter)

Random Search

Exercise S05.01

Using KDDCup99 dataset to build ML models for:

- Anomaly Detection with Isolation Forest
- Anomaly Detection with OC-SVM
- Choose one more ML algorithm for implementation and experiments.

Notes:

- For each model, determine which strategy is used? (Supervised ML, Semi-Supervised ML, Unsupervised ML?). Explain the capability of these approaches in real word scenarios?
- Evaluate the ML model's performance with common criteria, specific for Anomaly detection.
- Applying hyperparameter optimizing strategy for training mentioned models.

Exercise S05.02

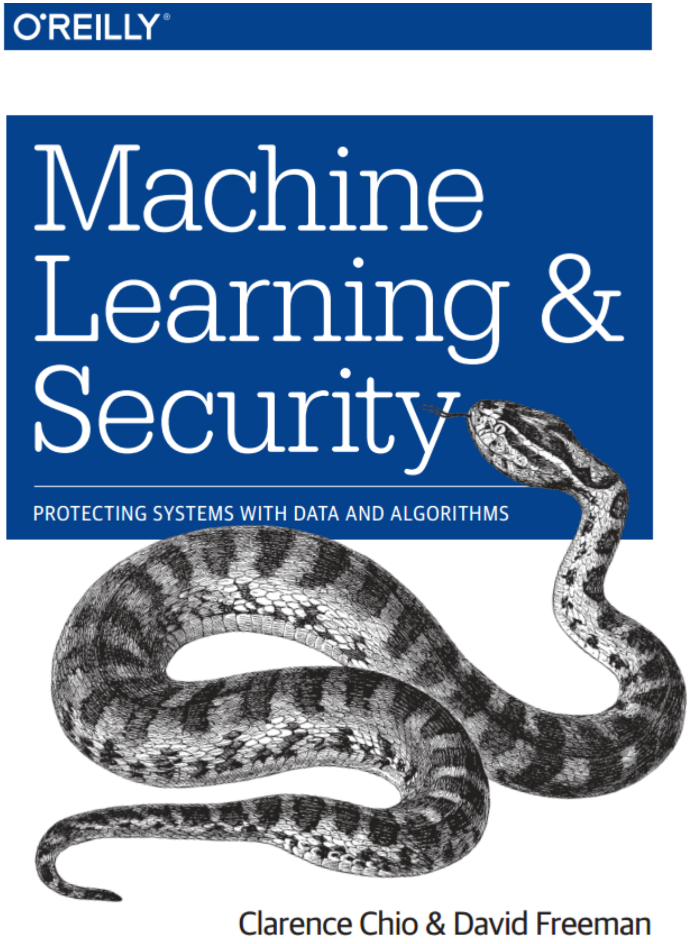
Build Host-based IDS using ML by your own:

- osquery, auditd: continuous and detailed introspection of your hosts
- Choose appropriate ML algorithms
- ADFA Intrusion Detection Datasets:
  - **The ADFA Linux Dataset (ADFA-LD)**
  - The ADFA Windows Dataset (ADFA-WD)
  - Link: https://research.unsw.edu.au/projects/adfa-ids-datasets

Reference for this topic…

Chapter 03 – Anomaly Detection, Book 00_Machine Learning and Security (O' Reilly).

Tài liệu tham khảo

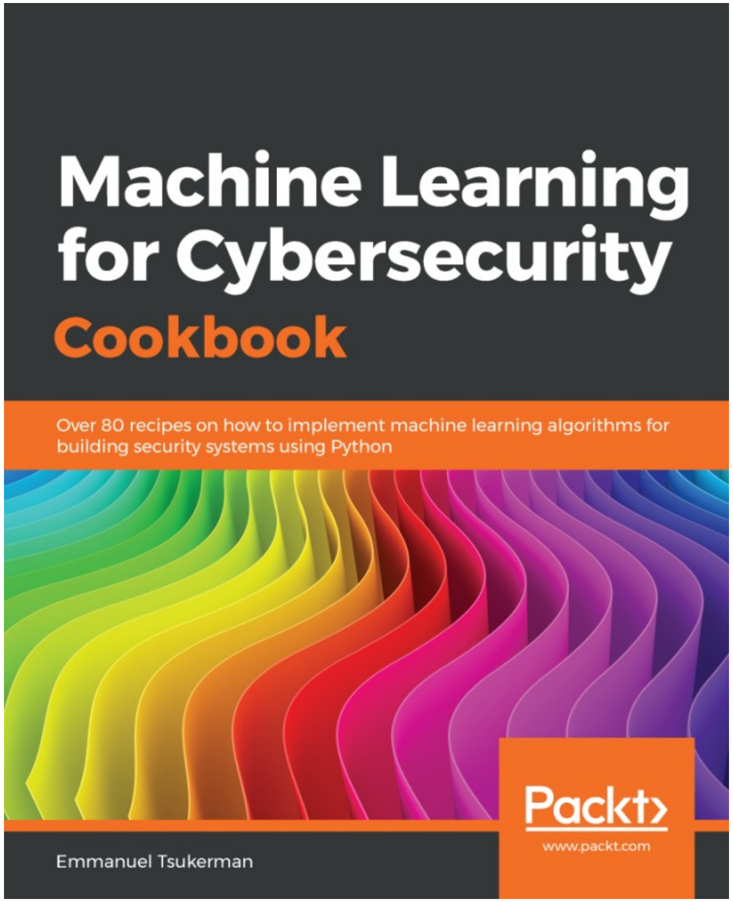


O'REILLY

Machine Learning & Security

PROTECTING SYSTEMS WITH DATA AND ALGORITHMS

Clarence Chio & David Freeman



Machine Learning for Cybersecurity Cookbook

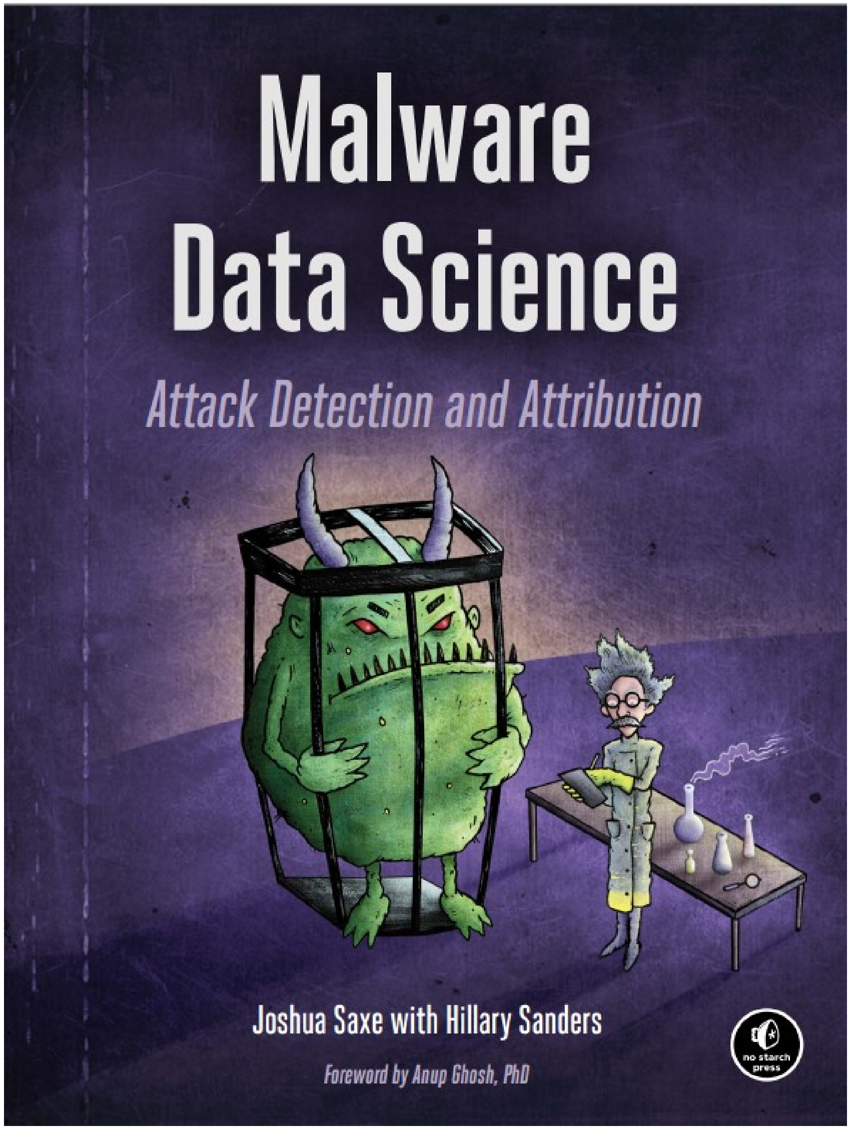
Over 80 recipes on how to implement machine learning algorithms for building security systems using Python

Emmanuel Tsukerman

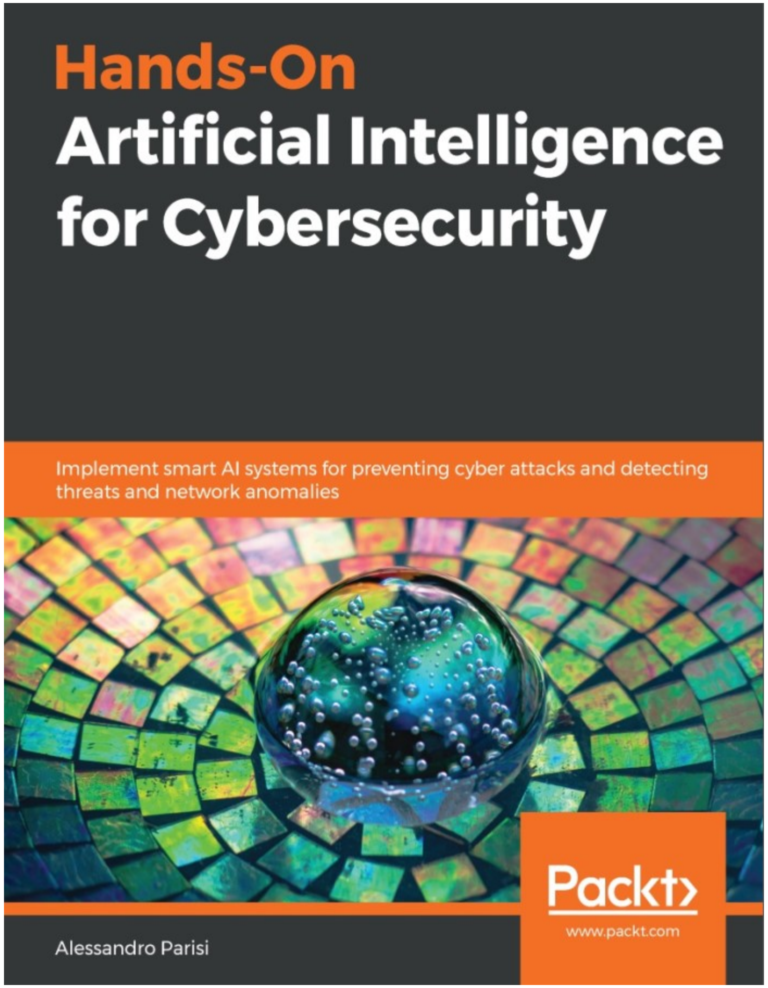
Packt

www.packt.com

Tài liệu tham khảo


Malware Data Science
Attack Detection and Attribution
Joshua Saxe with Hillary Sanders
Foreword by Anup Ghosh, PhD
no starch press

Tài liệu tham khảo

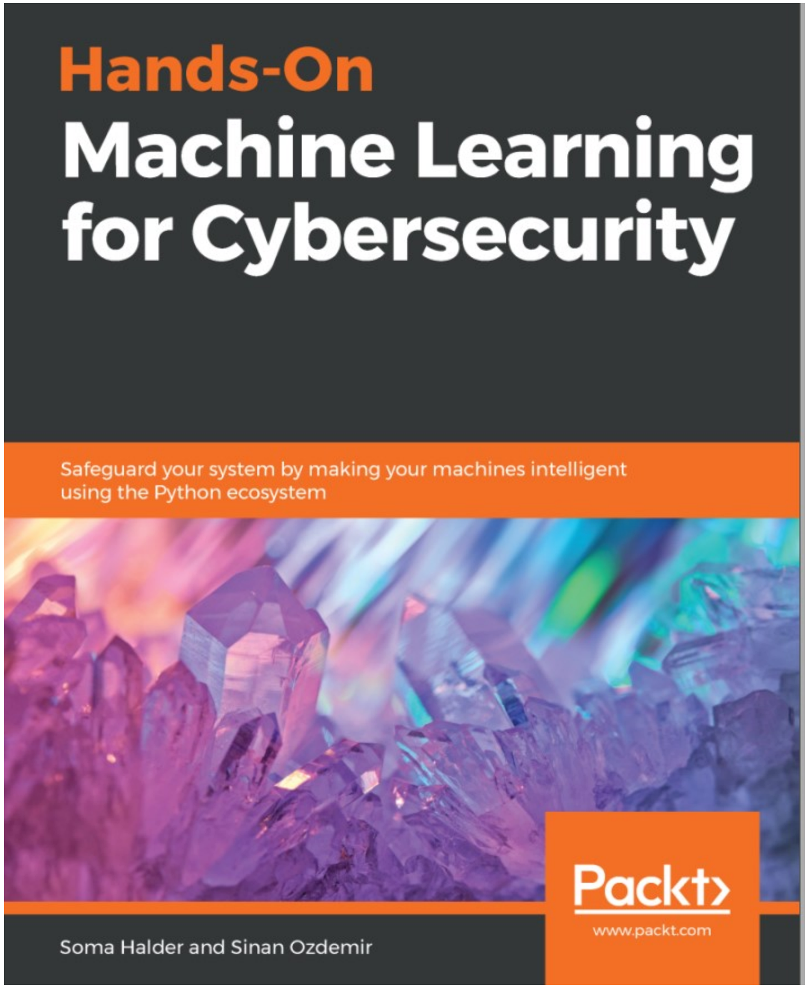


Hands-On
Artificial Intelligence for Cybersecurity

Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies

Packt> www.packt.com

Alessandro Parisi



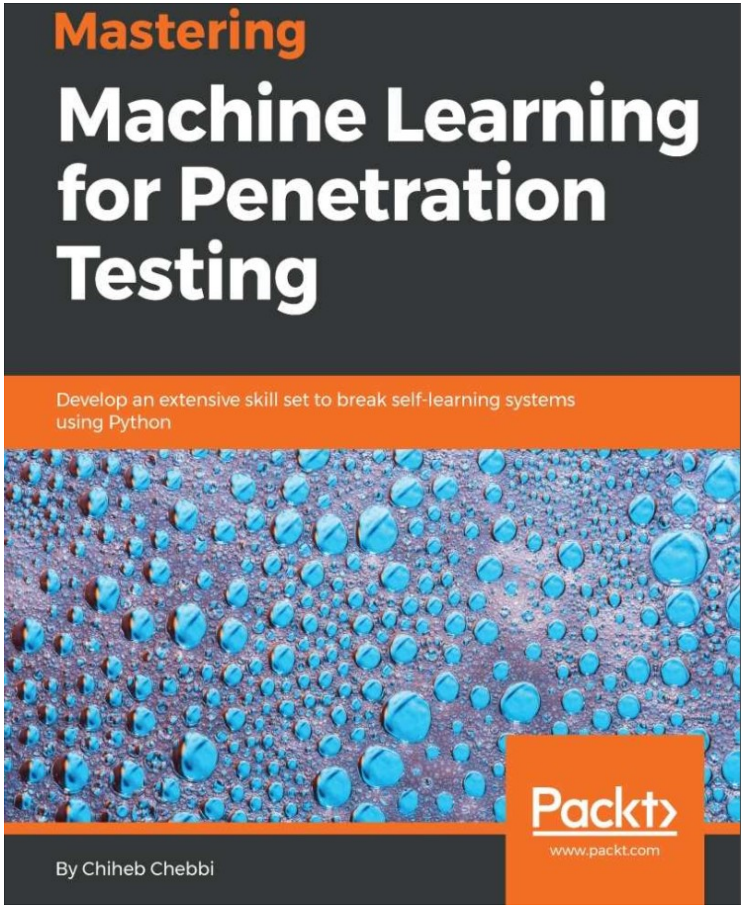
Hands-On
Machine Learning for Cybersecurity

Safeguard your system by making your machines intelligent using the Python ecosystem

Packt> www.packt.com

Soma Halder and Sinan Ozdemir

Tài liệu tham khảo

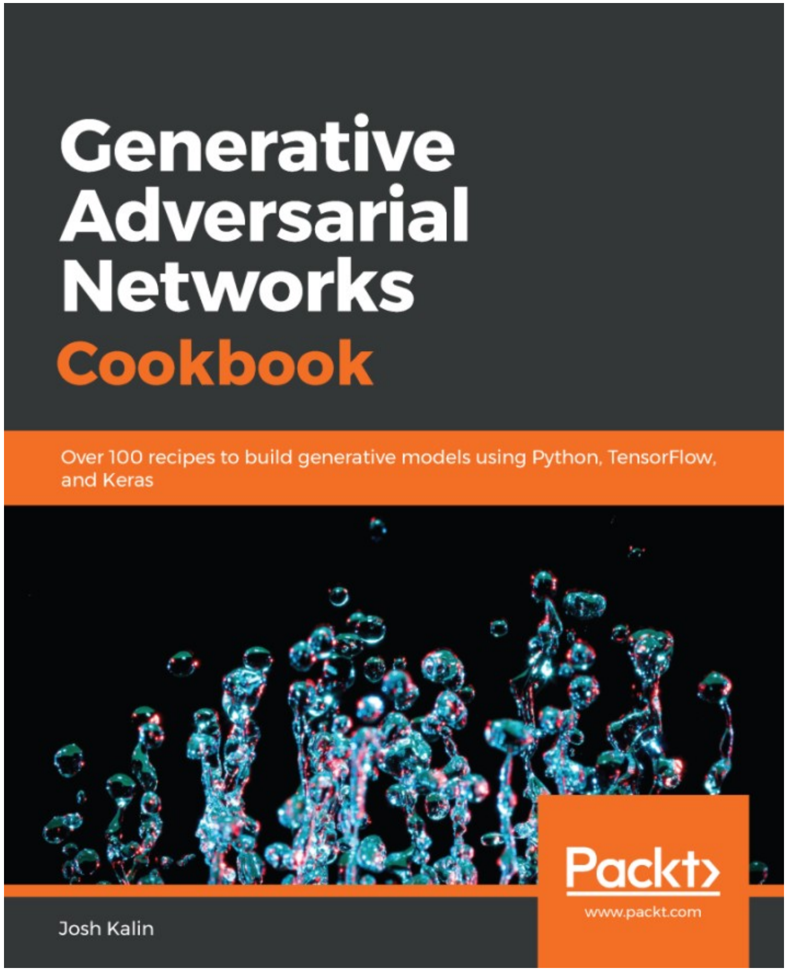


Mastering Machine Learning for Penetration Testing

Develop an extensive skill set to break self-learning systems using Python

Packt> www.packt.com

By Chiheb Chebbi



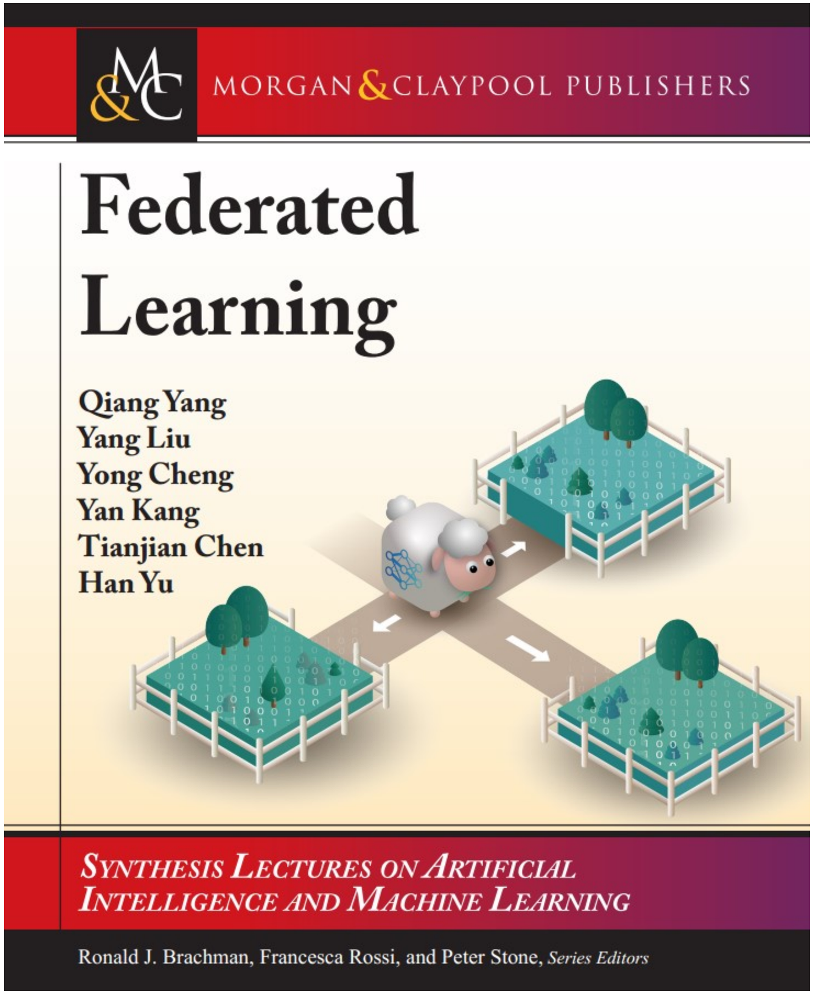
Generative Adversarial Networks Cookbook

Over 100 recipes to build generative models using Python, TensorFlow, and Keras

Josh Kalin

Packt> www.packt.com

Tài liệu tham khảo



MORGAN & CLAYPOOL PUBLISHERS

Federated Learning

Qiang Yang
Yang Liu
Yong Cheng
Yan Kang
Tianjian Chen
Han Yu

Synthesis Lectures on Artificial Intelligence and Machine Learning

Ronald J. Brachman, Francesca Rossi, and Peter Stone, *Series Editors*

Tài liệu tham khảo

1. Clarence Chio, David Freeman (2018). *Machine Learning and Security*. O'Reilly Media, Inc.
2. Emmanuel Tsukerman (2019), *Machine Learning for Cybersecurity Cookbook*. Packt Publishing.
3. Soma Halder, Sinan Ozdemir (2018), *Hands-On Machine Learning for Cybersecurity*, Packt Publishing.

Tài liệu tham khảo

1. Your First Machine Learning Project in Python Step-By-Step, https://machinelearningmastery.com/machine-learning-in-python-step-by-step/
2. Machine Learning Crash Course, https://developers.google.com/machine-learning/crash-course
3. How to Develop a GAN for Generating MNIST Handwritten Digits, https://machinelearningmastery.com/how-to-develop-a-generative-adversarial-network-for-an-mnist-handwritten-digits-from-scratch-in-keras/
4. GANs from Scratch 1: A deep introduction. With code in PyTorch and TensorFlow, https://medium.com/ai-society/gans-from-scratch-1-a-deep-introduction-with-code-in-pytorch-and-tensorflow-cb03cdcdba0f
5. Federated Learning: Collaborative Machine Learning without Centralized Training Data, https://ai.googleblog.com/2017/04/federated-learning-collaborative.html
6. https://cset.georgetown.edu/wp-content/uploads/Machine-Learning-and-Cybersecurity.pdf
7. http://web.stanford.edu/class/cs259d/#lectures
8. https://www.malwaredatascience.com/
9. https://github.com/oreilly-mlsec/book-resources

Môn học:

Phương pháp học máy trong an toàn thông tin

INSECLAB

Trường ĐH CNTT TP. HCM