

21.08.10



# Anomaly Detection

# 1 / Anomaly Detection 종류

# 학습 시 label 유무에 따른 분류

## 1. Supervised Anomaly Detection



- 학습시, Labeling된 정상/비정상 데이터를 모두 사용한 경우
- **Class-Imbalance(불균형)** 문제
- 모델 성능 평가가 가능하다는 점에서 직관적일 수 있지만, 척도 선정에 주의
- 비정상 sample을 확보하는데 많은 시간과 비용이 든다

## 2. Semi-supervised (One-Class) Anomaly Detection



- 정상 sample만 이용해서 모델을 학습시키는 방법
- 정상 sample들을 둘러싸는 boundary를 설정하고, 이 boundary 밖에 있는 sample들을 모두 비정상으로 간주
- [One-Class SVM](#), [Deep SVDD](#) 논문이 잘 알려져있음

## 3. Unsupervised Anomaly Detection



- 대부분의 데이터가 정상 sample이라는 가정하에 차원을 축소하고 복원을 하는 과정으로 비정상을 검출하는 방법이 대표적
- 모델 학습 후, 정상/비정상 데이터의 구분에 대한 임계치 설정이 필요할 수 있음
- 적합이 잘 된다면 정상/비정상 데이터의 모델링 후 분포가 이질적으로 나타날 수 있음

## Semi-supervised (One-Class) Anomaly Detection 관련논문

- Energy-based 방법론

["Deep structured energy based models for anomaly detection, 2016 ICML"](#)

- Deep Autoencoding Gaussian Mixture Model 방법론

["Deep autoencoding gaussian mixture model for unsupervised anomaly detection, 2018 ICLR"](#)

- Generative Adversarial Network 기반 방법론

["Anomaly detection with generative adversarial networks, 2018 arXiv"](#)

- Self-Supervised Learning 기반

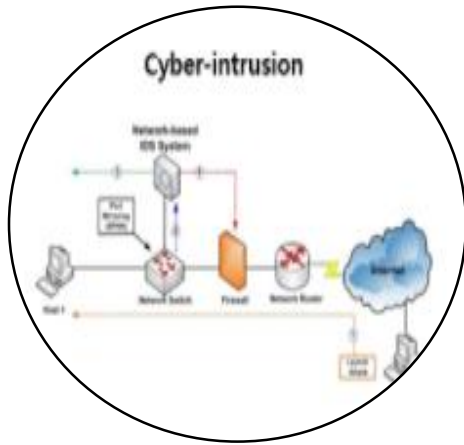
["Deep Anomaly Detection Using Geometric Transformations, 2018 NeurIPS"](#)

## Unsupervised Anomaly Detection 관련논문

- [Improving Unsupervised Defect Segmentation by Applying Structural Similarity to Autoencoders](#)
- [Deep Autoencoding Models for Unsupervised Anomaly Segmentation in Brain MR Images](#)
- [MVTec AD – A Comprehensive Real-World Dataset for Unsupervised Anomaly Detection](#)

## 2 / Anomaly Detection 적용 사례

## Anomaly Detection 적용사례



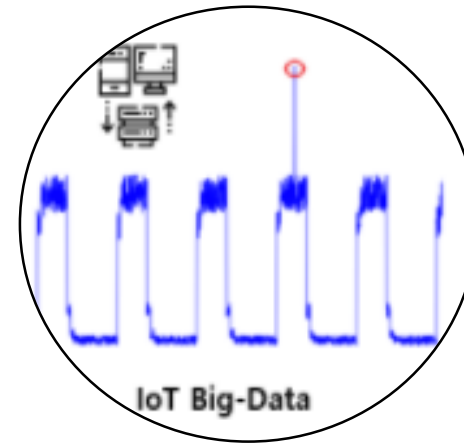
### Cyber-Intrusion Detection

컴퓨터 시스템 상에 일련의  
시계열 데이터에 대해  
이상치를 검출하여 침입을  
탐지함



### Fraud Detection

보험, 신용, 금융 관련  
데이터에서 불법 행위를  
검출하는 사례



### IoT Big-Data Anomaly Detection

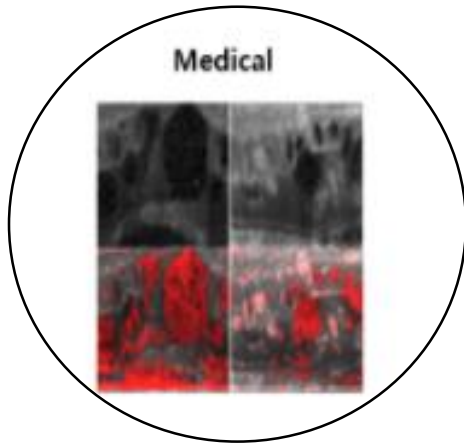
센서들로부터 생성된 데이터에  
대해 이상치를 탐지하는 사례



### Social Networks Anomaly Detection

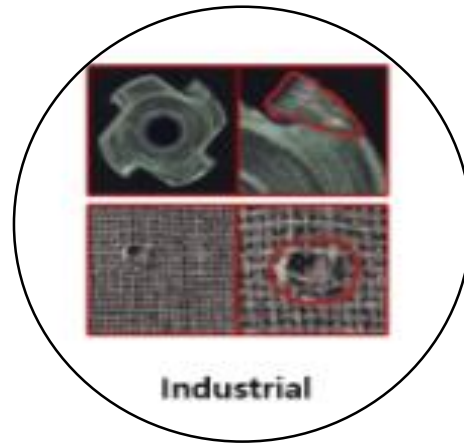
Text를 통해 스팸 메일, 비매너  
이용자, 허위 정보 유포자 등을  
검출

# Anomaly Detection 적용사례



## Cyber-Intrusion Detection

의료 영상, 뇌파 기록 등의 의학  
데이터에 대한 이상치 탐지



## Industrial Anomaly Detection

제조업 데이터에 대한  
이상치를 탐지하는 사례



## Log Anomaly Detection

시스템이 기록한 log를 보고  
실패 원인을 추적하는 사례



## Video Surveillance

비디오 영상에서 이상한  
행동이 발생하는 것을  
모니터링하는 사례

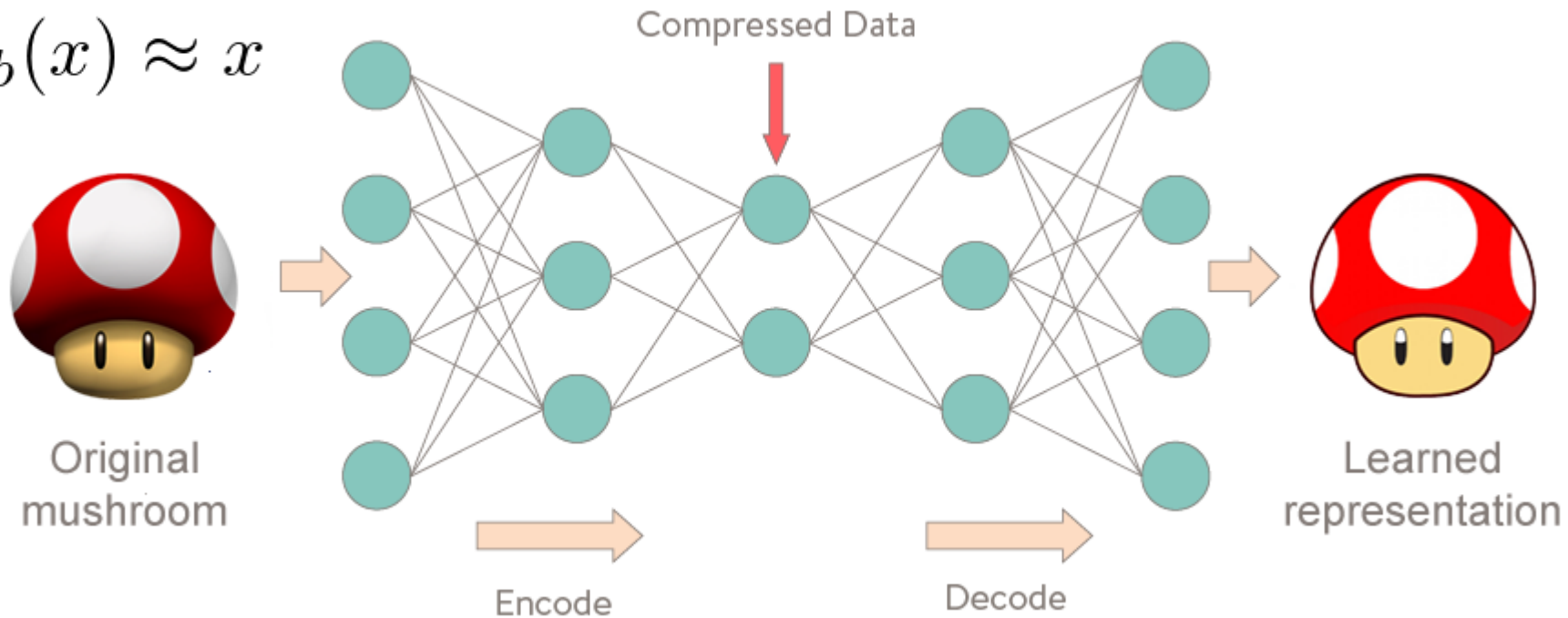
3 /

Autoencoder based  
Anomaly Detection



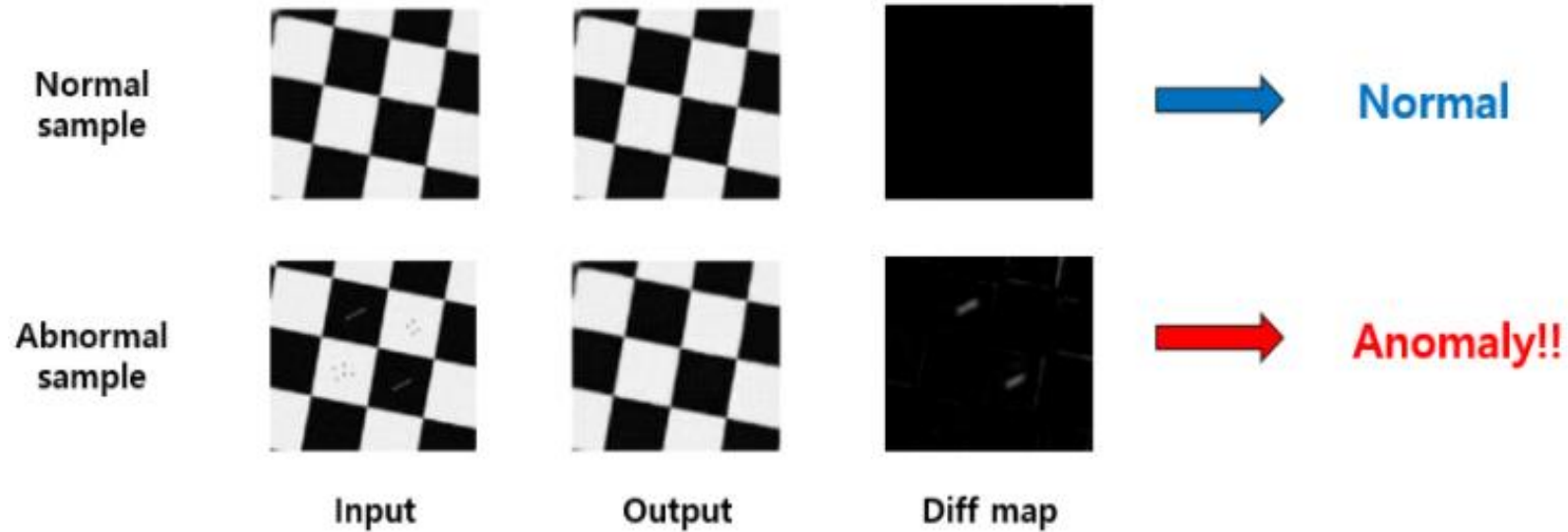
# Autoencoder based Anomaly Detection

$$f_{W,b}(x) \approx x$$



- 왼쪽에 있는 항은 입력값인  $x$ 가 신경망에 들어가는 것을 의미하며, 그 결과가 오른쪽에 있는  $x$ 와 같아지도록 근사하는 것
- 즉 Autoencoder란 '입력값  $x$ 를 받아서 다시 입력값  $x$ 를 결과로 뱉어내는 함수'
- Autoencoder는 입력을 latent variable로 압축하는 Encoding구조를 가지며 이는 데이터의 압축된 표상(representation)을 학습시키고 그 구조(structure)를 찾는 과정이다. 이는 은닉 유닛(hidden unit)의 수를 제한하는 방법을 통해 가능
- 이를 다시 원본과 가깝게 복원해내는 Decoding 과정으로 진행

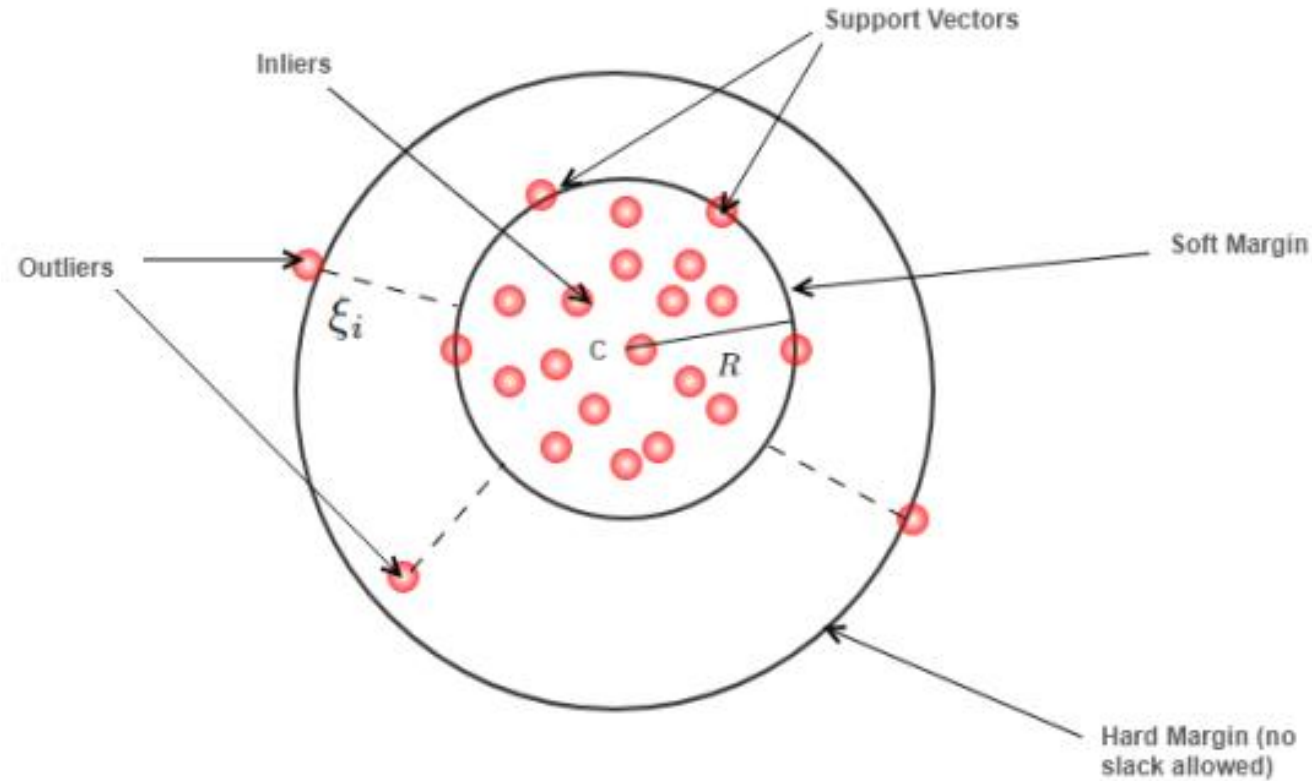
# Unsupervised Anomaly Detection



- 입력 샘플을 인코더를 통해 저차원으로 압축
- 압축된 샘플을 디코더를 통과시켜 다시 원래의 차원으로 복원
- 입력 샘플과 복원 샘플의 복원 오차(reconstruction error) 계산
- 복원 오차는 이상 점수(anomaly score)가 되어 threshold와 비교를 통해 이상 여부를 결정
  - threshold 보다 클 경우 이상으로 간주
  - threshold 보다 작을 경우 정상으로 간주

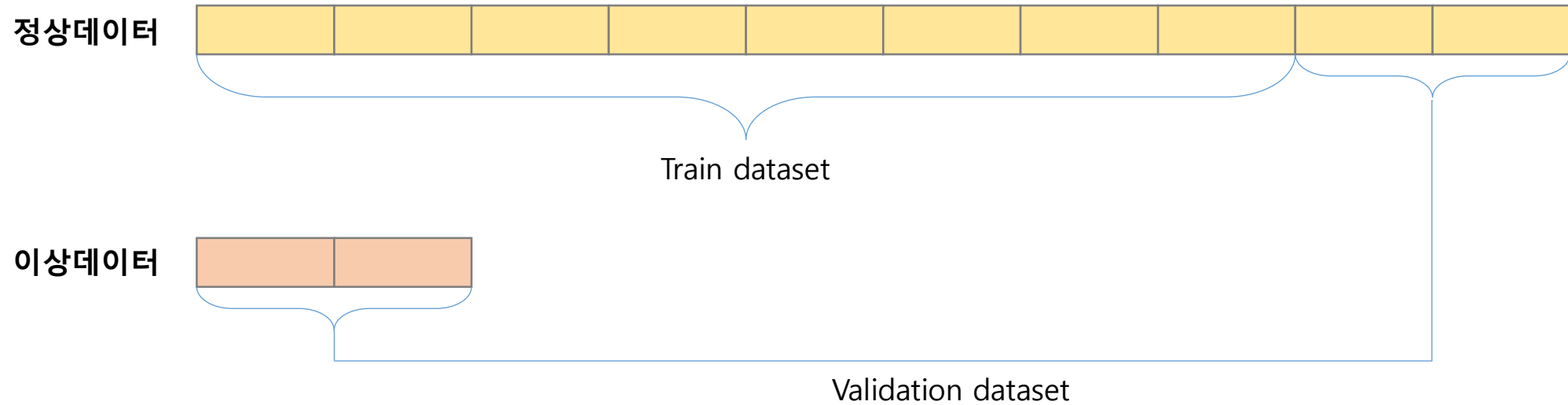
# 4 / One-class SVM

# One-Class SVM



- 주어진 데이터를 잘 설명할 수 있는 최적의 support vector를 구하고 이 영역 밖의 데이터들은 outlier로 간주하는 방식으로 이상치 탐지, 이미지 검색, 문서/ 텍스트 분류 등에 사용
- One class svm은 기본적으로 SVDD에서 파생되었다. SVDD에서는 모든 데이터를 고차원 공간으로 매핑한 다음 대부분의 데이터가 내부에 있도록 한다.
- 위의 그림에서 센터인  $c$ 로부터의 거리가  $R$ 보다 큰 경우를 모두 이상치로 판단한다.

# One-Class SVM



- one-class svm 은 정상데이터만을 이용해 학습시키고, 이상탐지에 관한 성능을 확인하기 위해서 정상데이터를 분할하여 train dataset을 만든다.
- 정상데이터 중 train dataset이 아닌 데이터와 이상치 데이터를 결합해 validation dataset으로 활용하는 경우가 많다.



## reference

- [https://velog.io/@vvakki\\_/Anomaly-Detection%EC%9D%B4%EC%83%81%EC%B9%98-%ED%83%90%EC%A7%80%EB%9E%80](https://velog.io/@vvakki_/Anomaly-Detection%EC%9D%B4%EC%83%81%EC%B9%98-%ED%83%90%EC%A7%80%EB%9E%80)
- <https://hoya012.github.io/blog/anomaly-detection-overview-1/>