DEVIEW
2019

Operational AI: 지속적으로 학습하는 Anomaly Detection 시스템 만들기

김기현
MakinaRocks
MAKINA ROCKS

CONTENTS

DEVIEW 2019

DEVIEW
2019

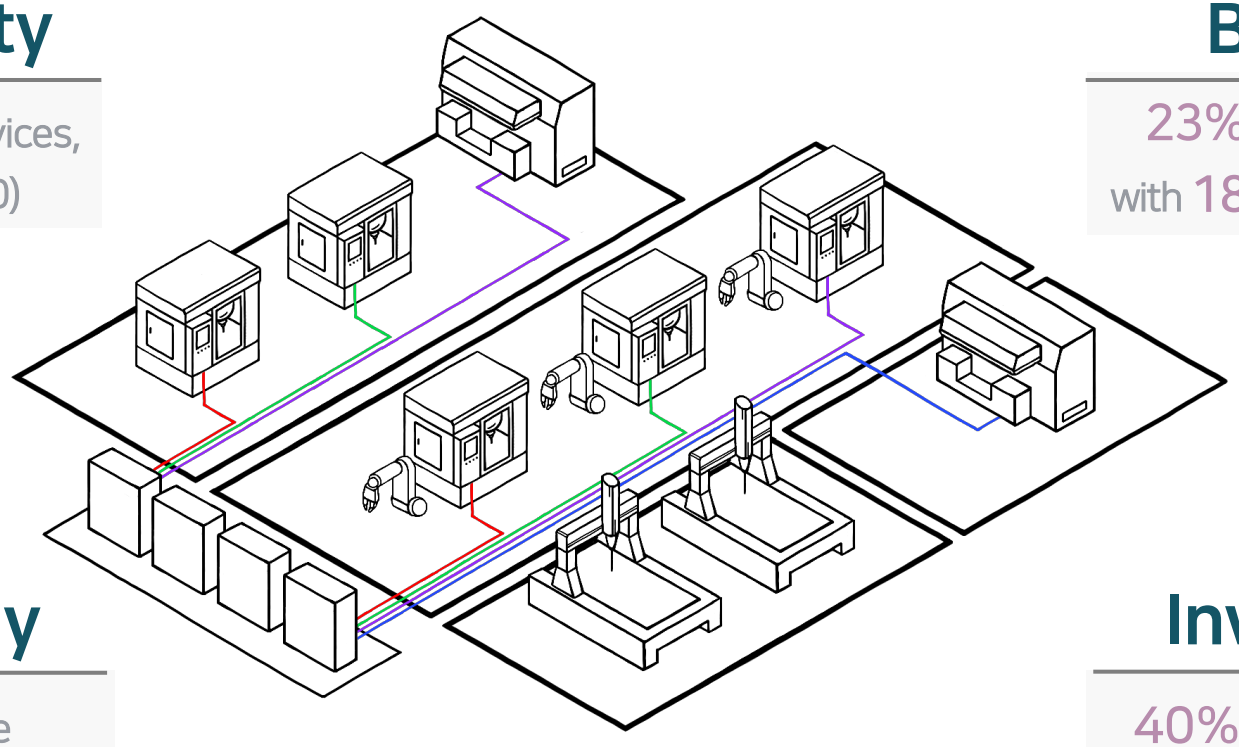
1. Introduction to Industrial Artificial Intelligence

제조업을 비롯한 산업내 AI 기술의 적용

DEVIEW 2019

Connectivity

50B+ Connected devices,
600 ZB/yr (by 2020)



Benefits

23% revenue increase
with 18% reduction in cost

Technology

10M+ learnable
parameters in a Deep
Learning architecture

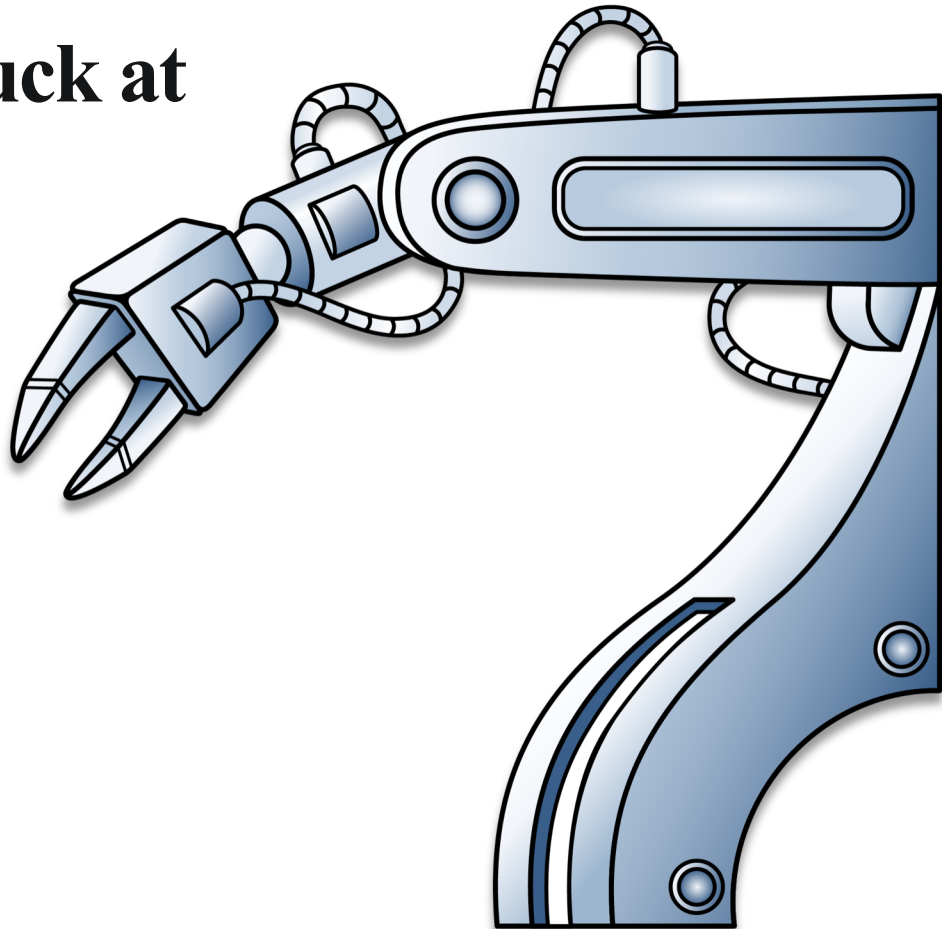
Investment

40% CAGR with $17B+
market in 2025
(AI in Manufacturing)

하지만 현실은…

Almost 2 in 3 companies that are adopting digital manufacturing solutions find themselves stuck at the pilot phase.

#McKinseyHM19 #HM19

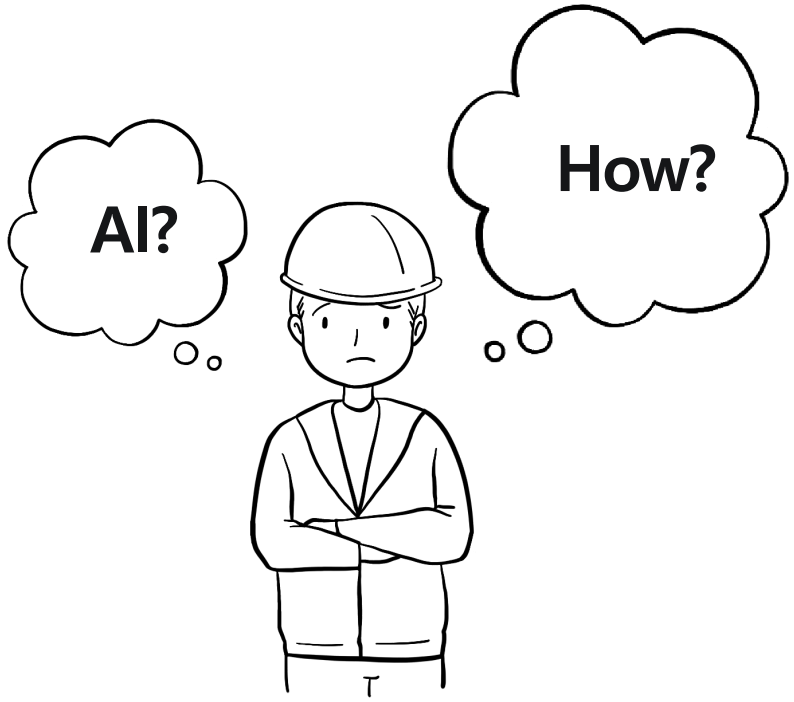


왜? – AI 도입에 대한 성공 경험 부족

DEVIEW 2019

성공 사례 및 경험 부족으로 인한 리스크 증가

사례의 부족으로 인한 문제 정의 어려움

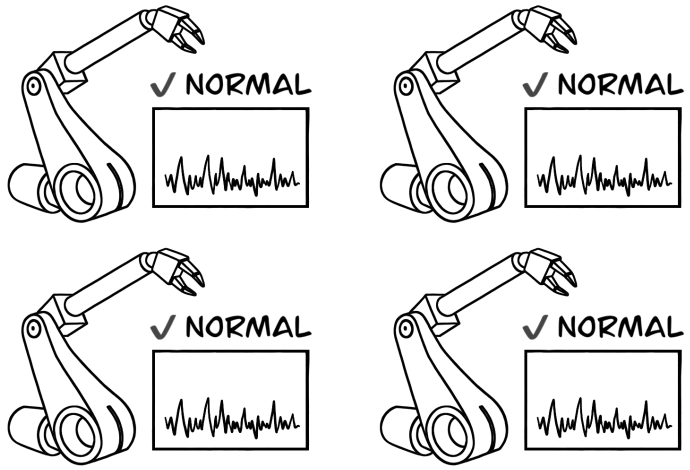


선행 비용 발생으로 인한 리스크 증가

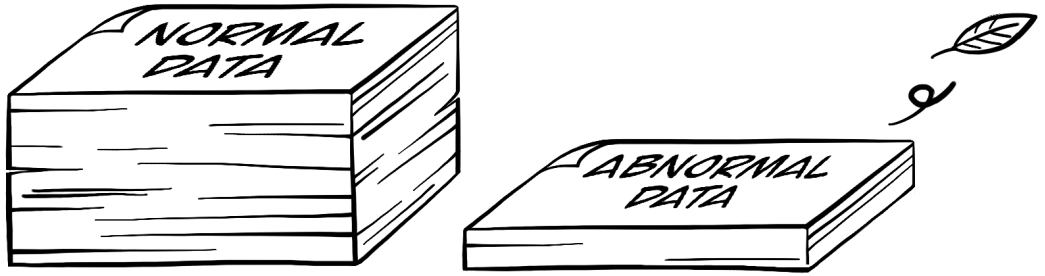
왜? – 레이블 불균형의 문제

레이블 불균형으로 인해 일반적인 분류 알고리즘을 적용하기 어려움

공장은 대부분 정상 동작



비정상 데이터가 학습에 기여하는 부분이 작아 학습이 어려움

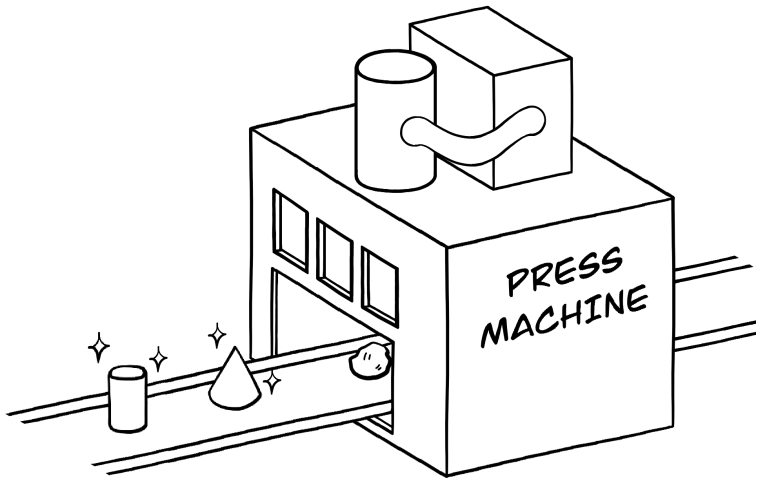


비정상 특징을 배우기에는 데이터가 부족함

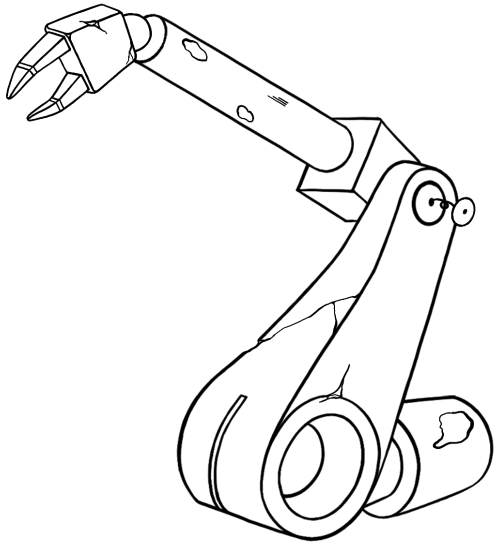
왜? – 지속적인 제조 공정의 변화

한번의 모델 학습으로는 계속되는 공정 환경 변화에 대응할 수 없음

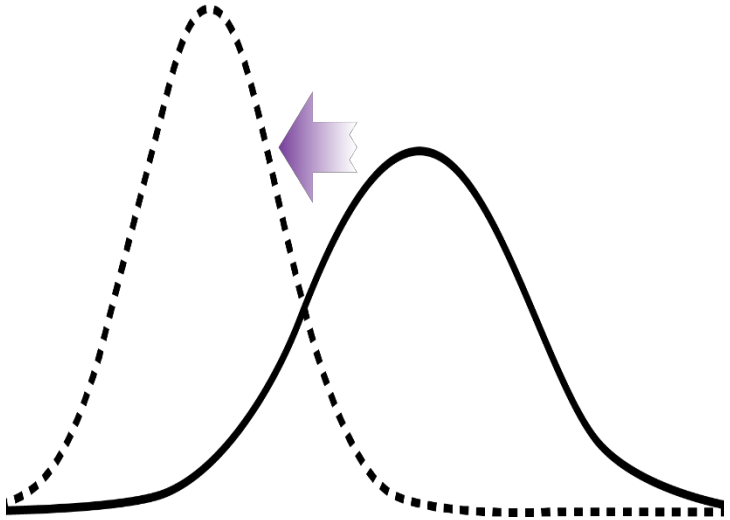
새로운 부품을 찍어내는 프레스 머신



기계 장비 노후화



입력 분포 변화

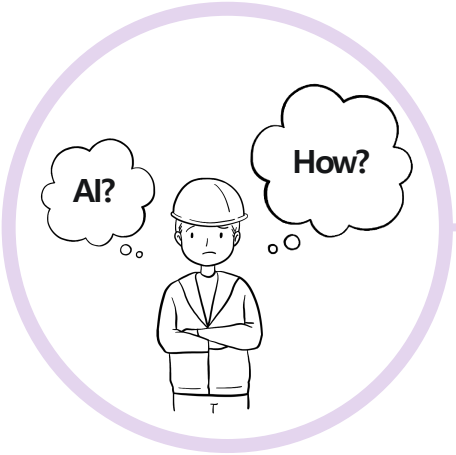


오늘의 주제

DEVIEW 2019

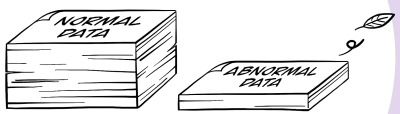
제조업 AI를 적용하기 위한 어려움과 해결방안 (feat. 로봇팔)

문제 정의 단계



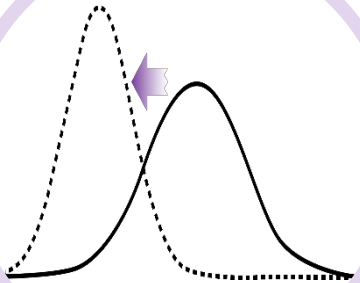
- 복잡도의 증가, 높아진 기대치
- 사례부족으로 인한 리스크

모델 개발 측면



- 비직관적인 데이터
- 레이블 불균형 + 노이즈 레이블

모델 운영 측면



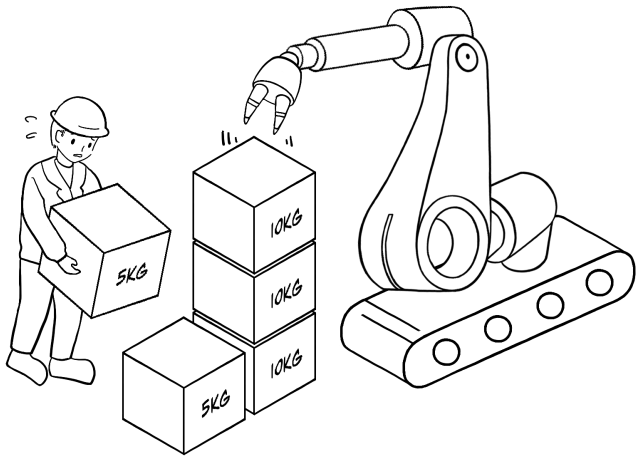
- 지속적인 학습
- 모델 관리 등

현대 생산 공정에서 산업용 로봇의 역할

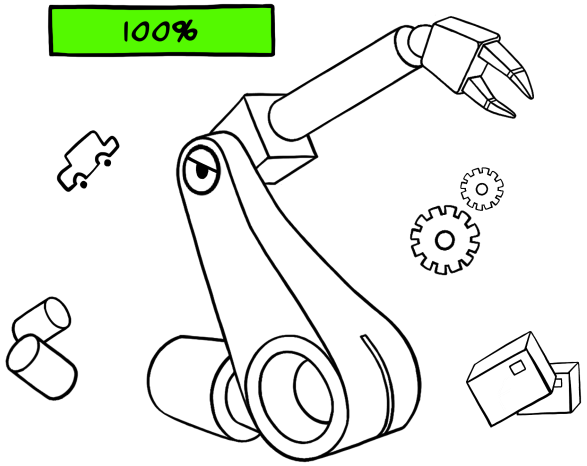
DEVIEW 2019

인건비 증가로 인한 산업용 로봇의 수요 증가

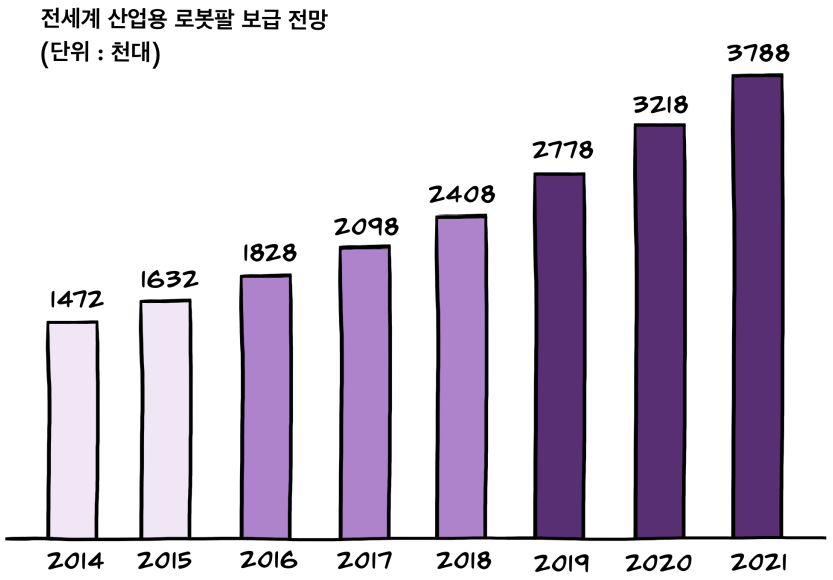
위험하고 어려운 작업



지치거나 실수하지 않음



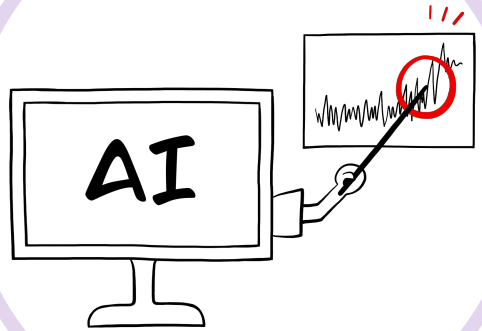
연도별 산업용 로봇 증가량



고장 시점을 미리 예측할 수 있다면?

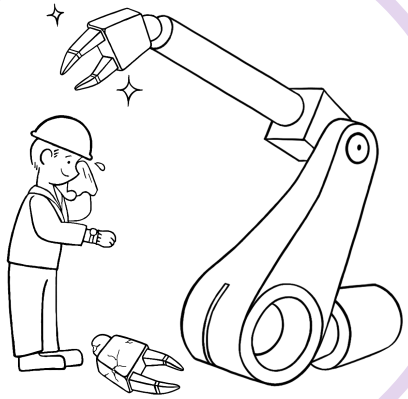
예상치 못한 가동 중지로 인한 손실 발생을 최소화

AI의 고장 징후 탐지

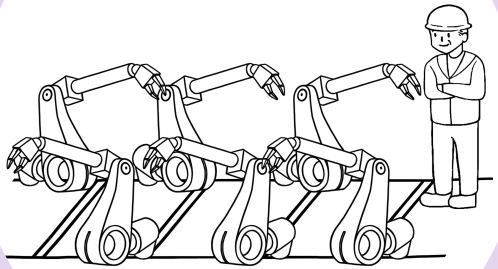


미리 부품 준비

미리/즉시 부품 교체



생산성 향상 / 비용 절감



2. Anomaly Detection:

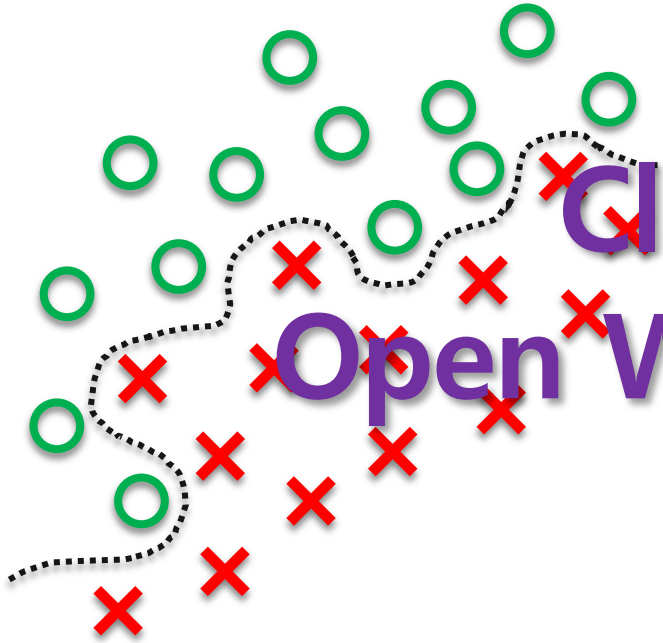
Reconstruction along Projection Pathway (RaPP)

Binary Classification?

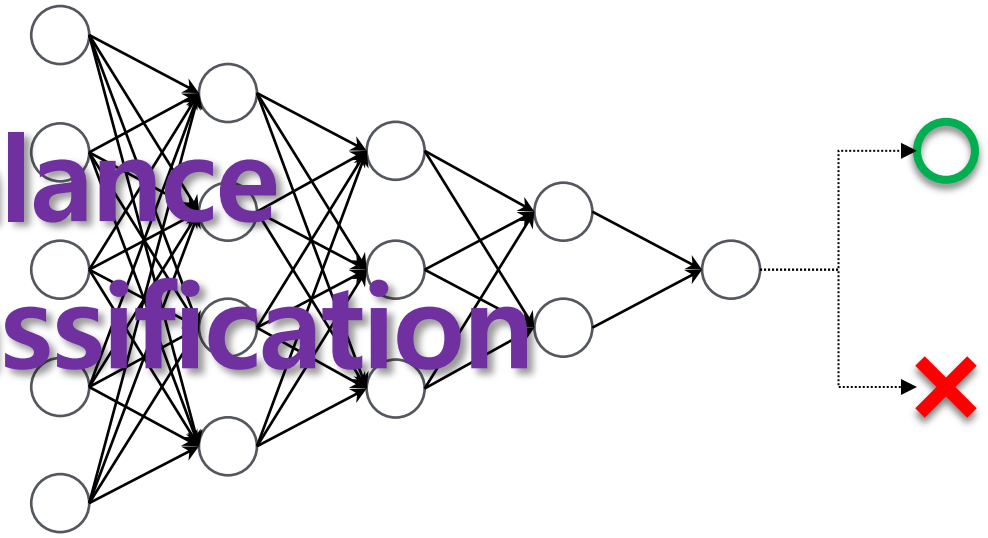
DEVIEW 2019

정상 데이터와 비정상 데이터를 분류하자?

정상 샘플과 비정상 샘플이 주어졌을 때,



이진 분류를 통해 정상과 비정상을 분류하자



Class Imbalance

Open World Classification

Novelty Detection

정상 데이터만을 학습한 후, 비정상 데이터를 걸러내자

비정상 데이터 확보 어려움
일반적인 분류 모델 적용 불가

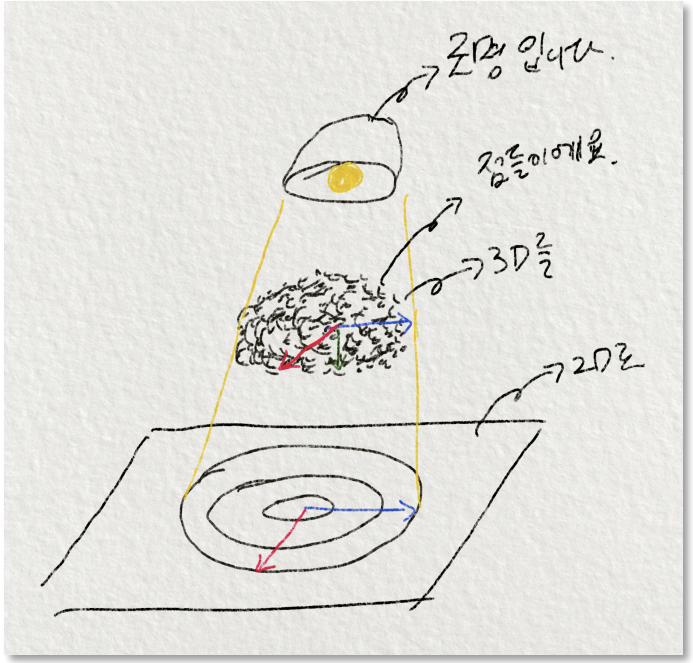
정상 데이터의 특징을 학습

학습된 특징이 관찰되지 않거나
새로운 특징이 나타날 경우
비정상 데이터로 간주

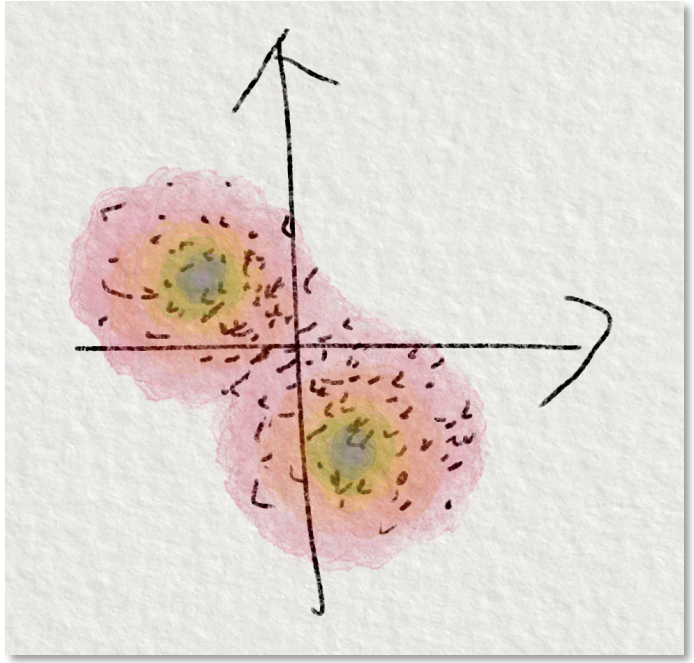
Previous Methods

정상 데이터의 범위를 정의하여 비정상 샘플을 가려내자

차원 축소를 통한 특징 추출 (feat. PCA)



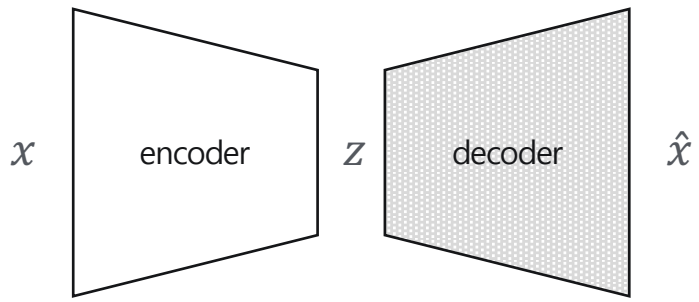
클러스터링을 통한 확률 분포 근사 (feat. GMM)



Deep Learning based Methods

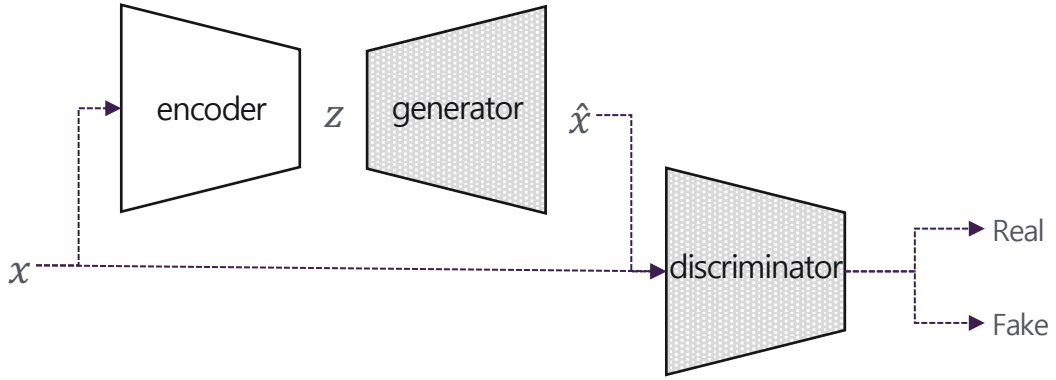
생성 모델을 통해 복원 오차가 클 경우 비정상 샘플로 간주

AE based methods



- 학습: 압축과 해제를 통해 특징 추출 방법을 학습
- 장점: 차원 축소 기능을 제공함.
  학습이 용이함.
- 단점: MSE 손실함수 사용으로 인해 복원 성능이 떨어짐.

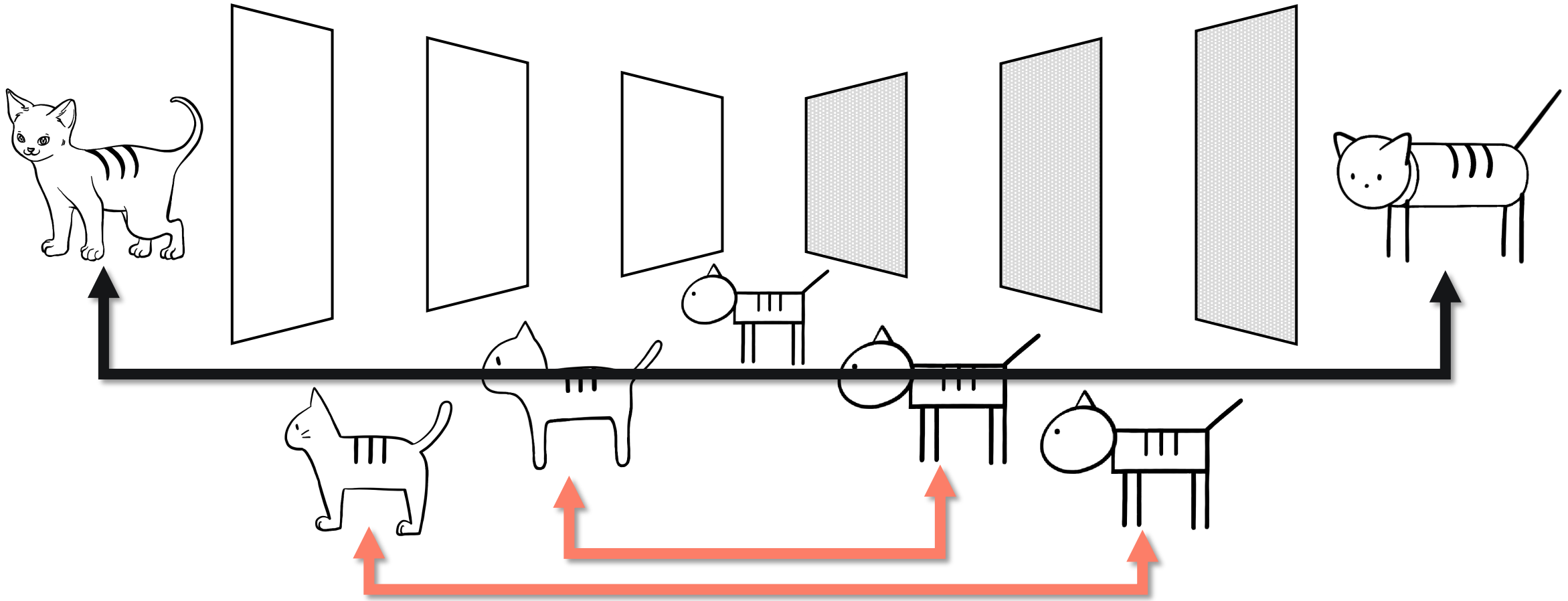
GAN based methods



- 학습: generator와 discriminator 훈련 후에,
  fix된 generator에 encoder를 붙임.
- 장점: MSE 손실함수에 비해 복원 성능이 향상 된다.
- 단점: Original GAN은 차원 축소 기능을 제공하지 않는다.
  학습이 불안정함.

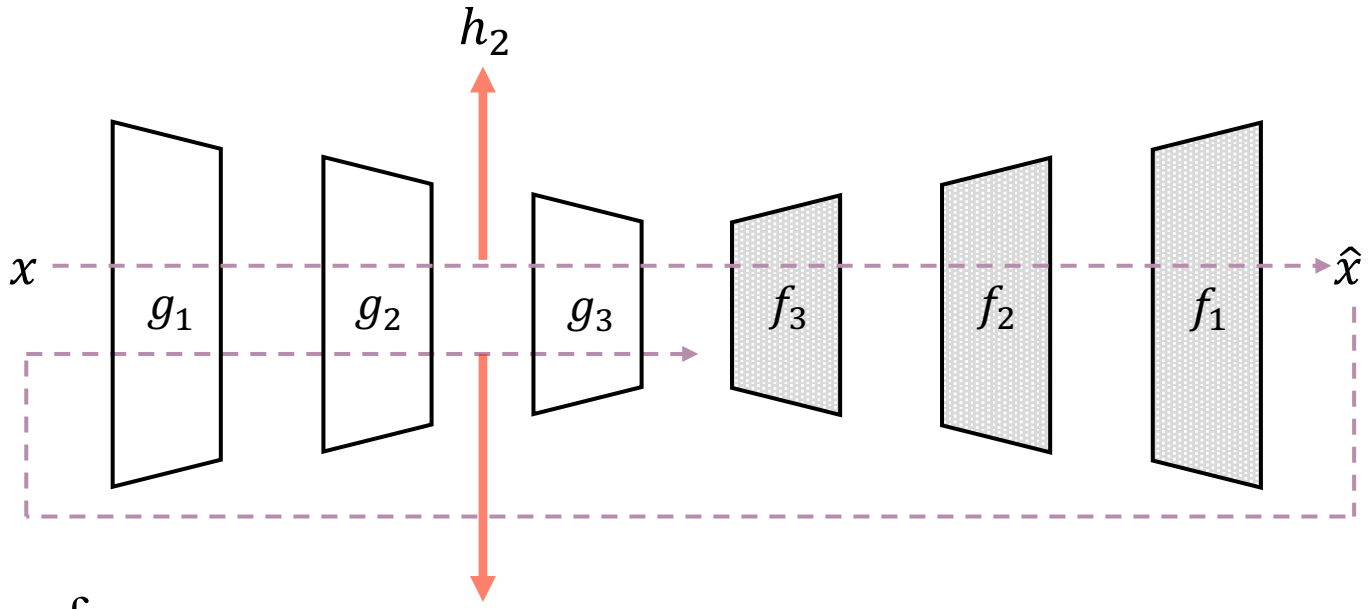
Motivation of RaPP

인코더와 디코더의 중간 결과물을 활용하여 성능을 높일 수 있을까?



RaPP

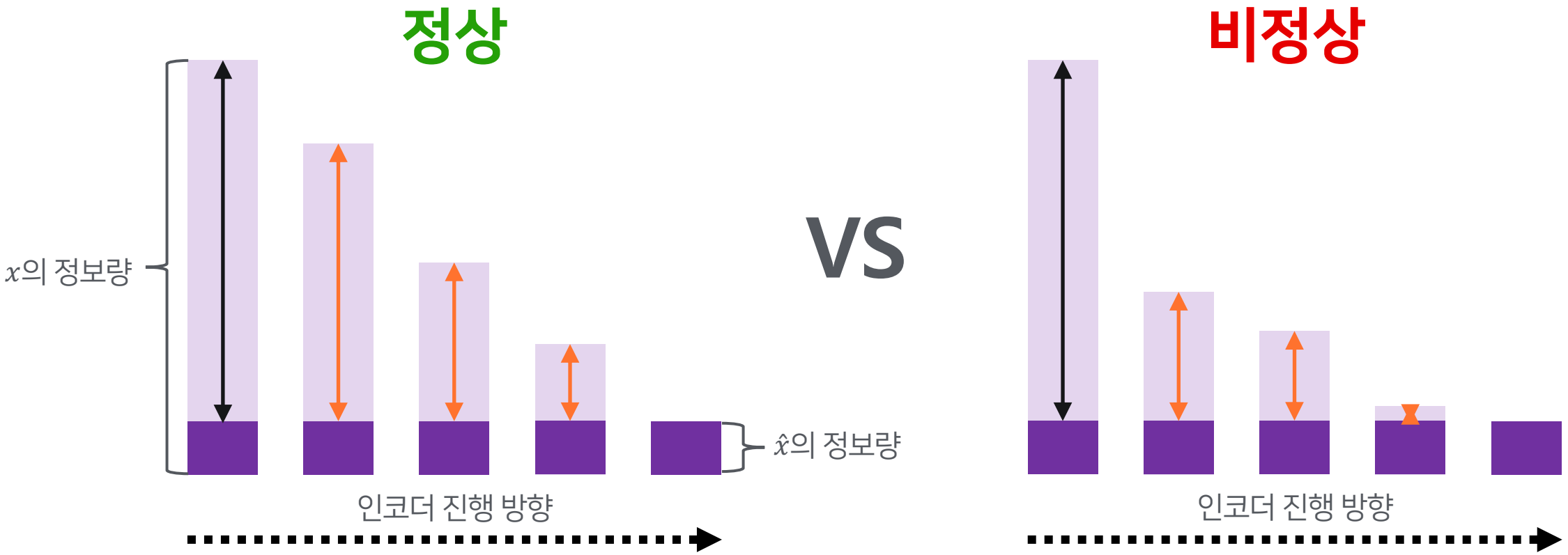
복원 샘플을 다시 인코더에 넣어보자



hidden representation of reconstruction of input $g_2 \circ g_1(\hat{x}) = \hat{h}_2$

2.7 RaPP – Intuition

레이어를 지나며 남아있는 정보량을 비교

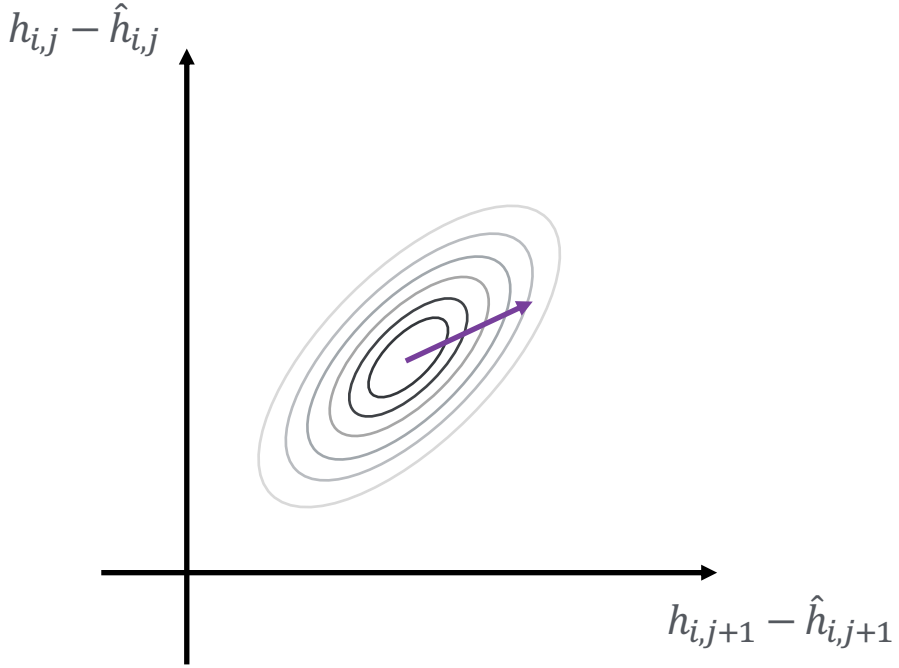


Normalized Aggregation

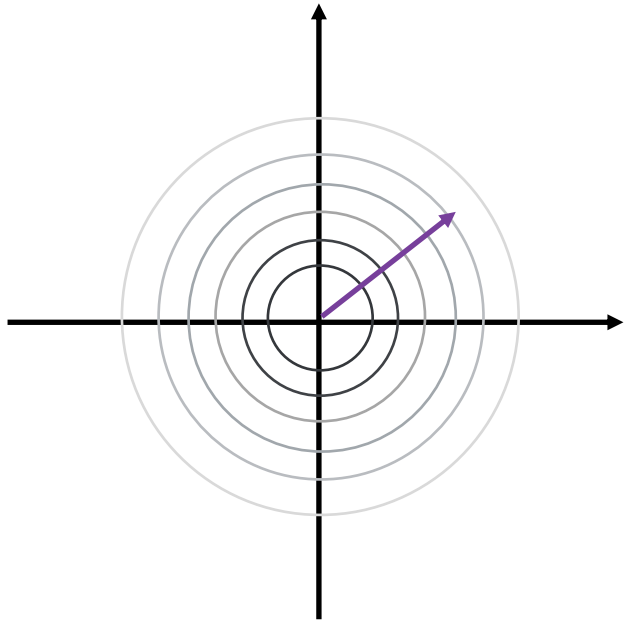
DEVIEW 2019

SVD를 통해 서로 다른 reconstruction error를 normalize

각 layer 별 hidden reconstruction error의 분포들을
하나의 차원으로 본 multivariate gaussian이라고 했을 때,



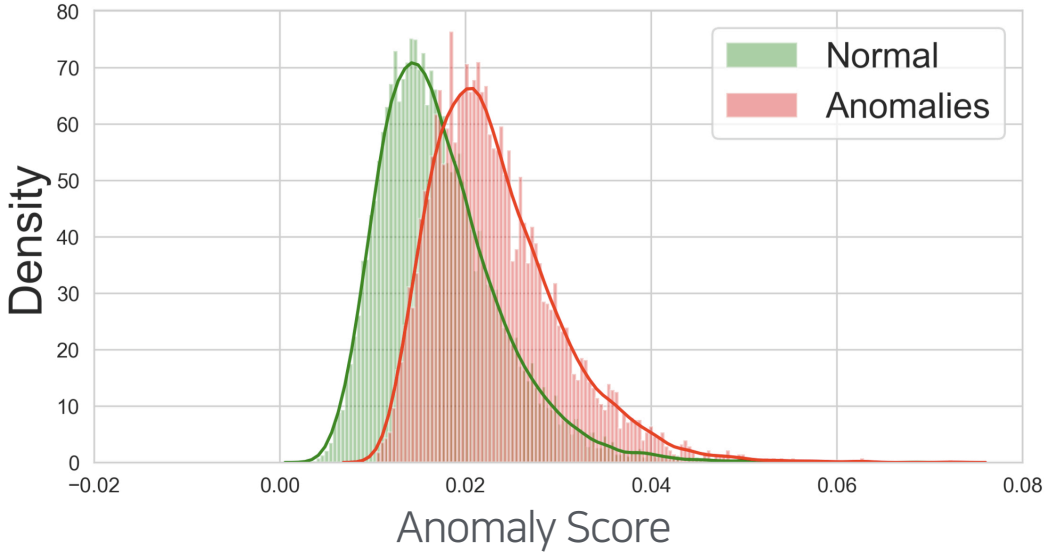
SVD를 통해 정규화된 unit-gaussian의 형태로 바꾸어
원점으로부터의 거리를 anomaly score로 활용



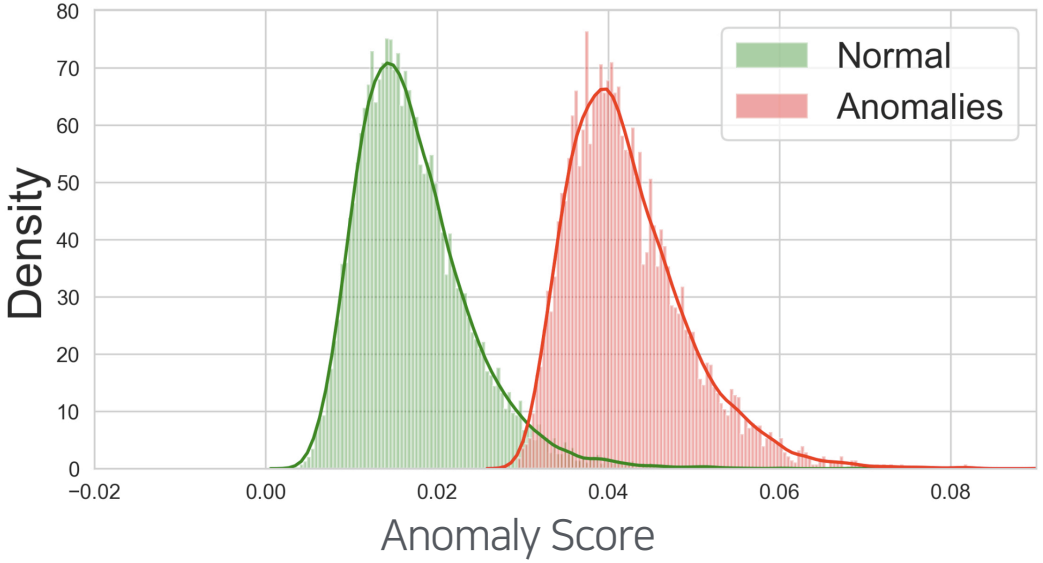
Evaluation Metric

AUROC를 통해 정상과 비정상 분포의 분리 정도를 측정

AUROC: 0.6

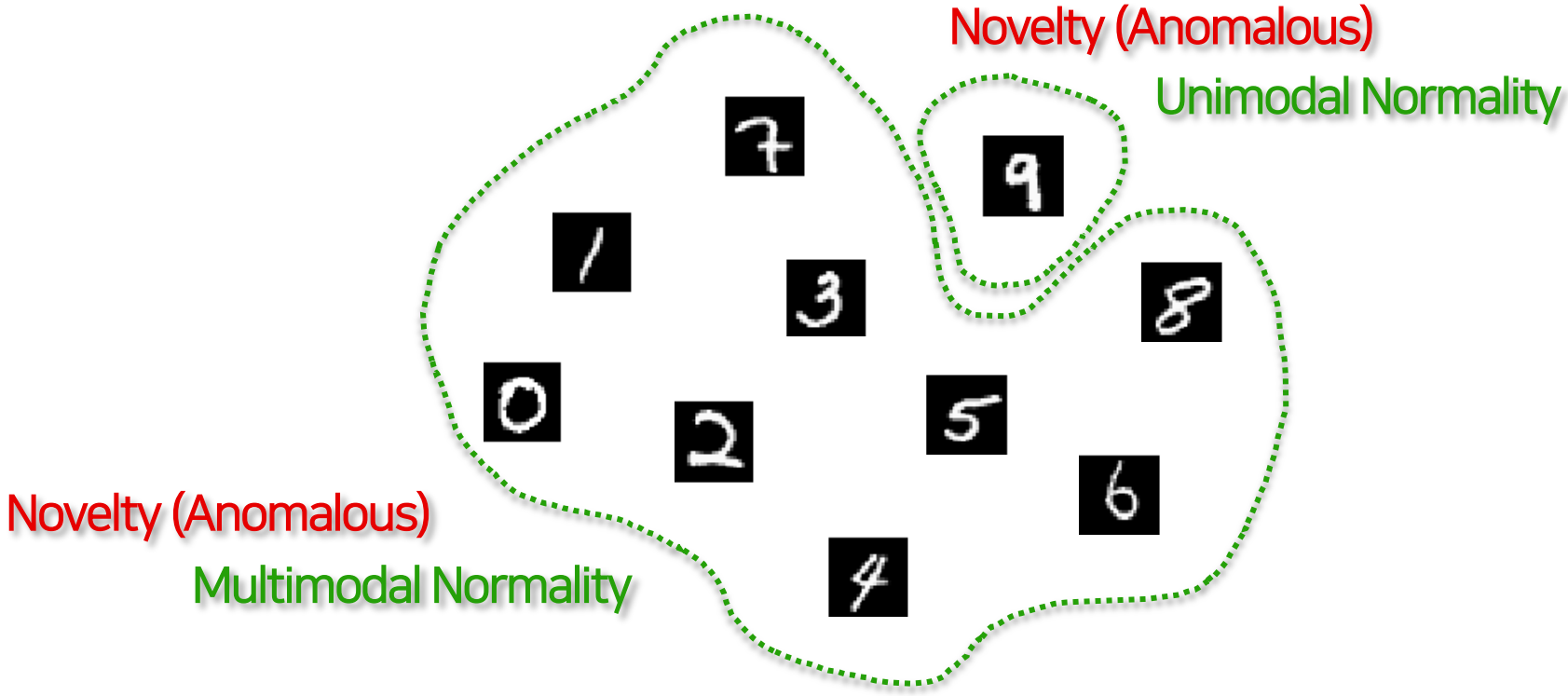


AUROC: 0.99



Experiment Setup

Multimodal / Unimodal normality case에 대해 실험을 수행

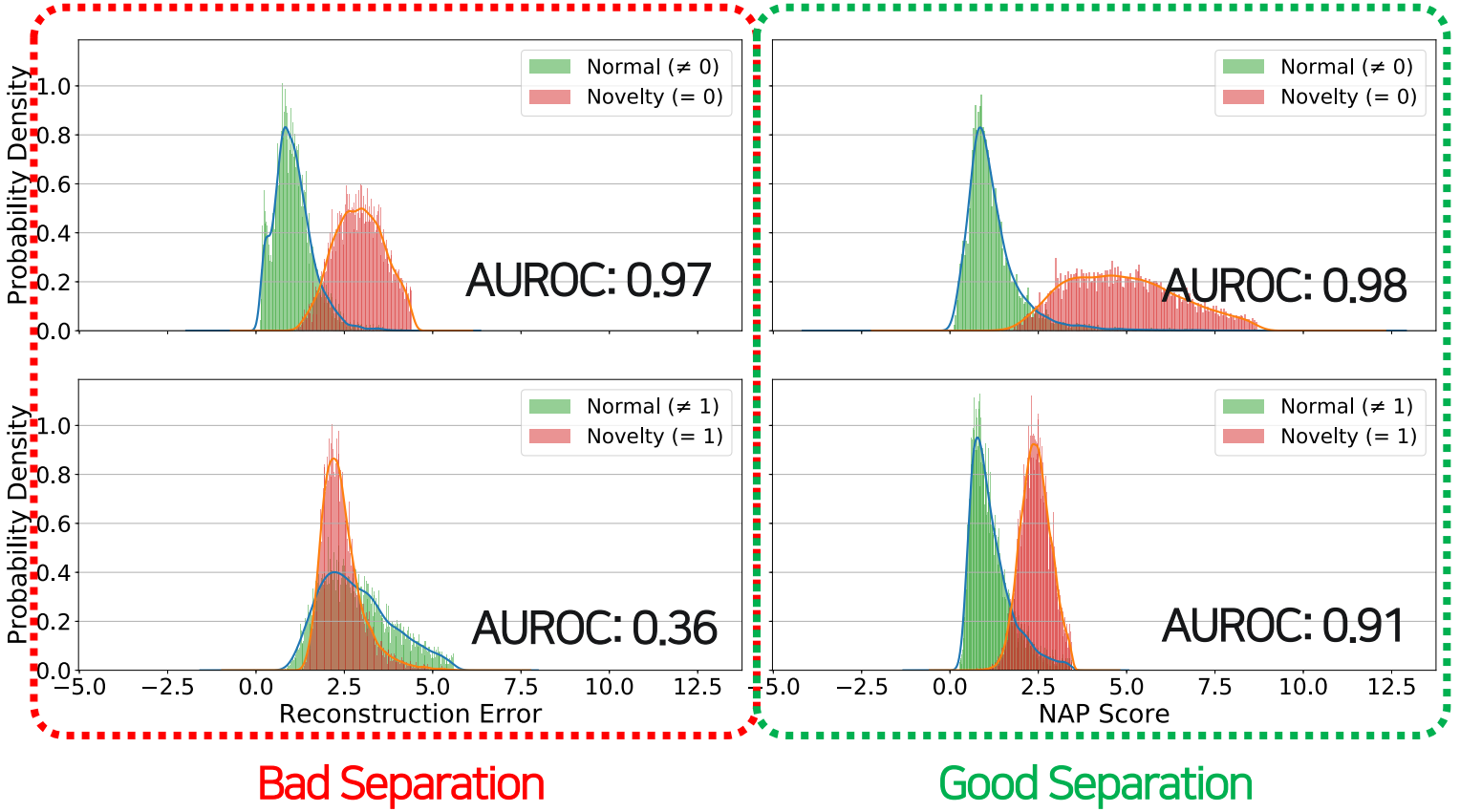


RaPP – Result

DEVIEW 2019

기존 방식보다 더 다양한 이상 샘플을 정확하게 탐지

Novelty Digit



RaPP – Evaluation

DEVIEW 2019

다양한 baseline과의 비교 실험을 통해 검증 하자.

NIPS 18 ICML 18 NIPS 18

Dataset	OCNN[1]	GPND[2]	DSVDD[3]	GT[4]	RaPP_{AE}	RaPP_{VAE}	RaPP_{AAE}
Multimodal Normality (Novelty Ratio: 35%)							
MNIST	0.600	0.501	0.622	0.893	0.899	0.927	**0.929**
F-MNIST	0.609	0.691	0.610	0.725	0.734	**0.737**	0.727
Unimodal Normality (Novelty Ratio: 50%)							
MNIST	0.927	0.971	0.922	0.974	**0.979**	0.976	0.977
F-MNIST	0.915	0.917	0.923	**0.935**	0.933	0.934	0.928

[1] Raghavendra Chalapathy, Aditya Krishna Menon, and Sanjay Chawla. Anomaly detection using one-class neural networks. arXiv preprint arXiv:1802.06360, 2018.

[2] Stanislav Pidhorskyi, Ranya Almohsen, and Gianfranco Doretto. Generative probabilistic novelty detection with adversarial autoencoders. In NeurIPS, pp. 6823–6834, 2018.

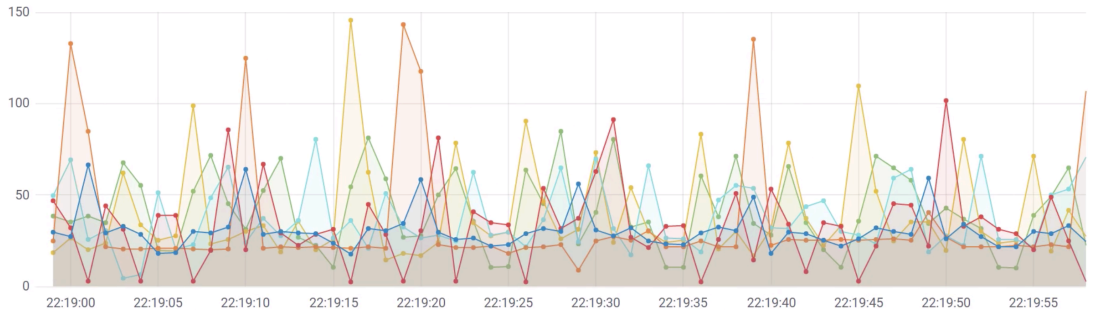
[3] Lukas Ruff, Robert Vandermeulen, Nico Goernitz, Lucas Deecke, Shoaib Ahmed Siddiqui, Alexander Binder, Emmanuel Muller, and Marius Kloft. Deep one-class classification. In ICML, 2018.

[4] Izhak Golan and Ran El-Yaniv. Deep anomaly detection using geometric transformations. NIPS, 2018

RaPP – Evaluation

DEVIEW 2019

다양한 데이터를 통해 검증 하자.

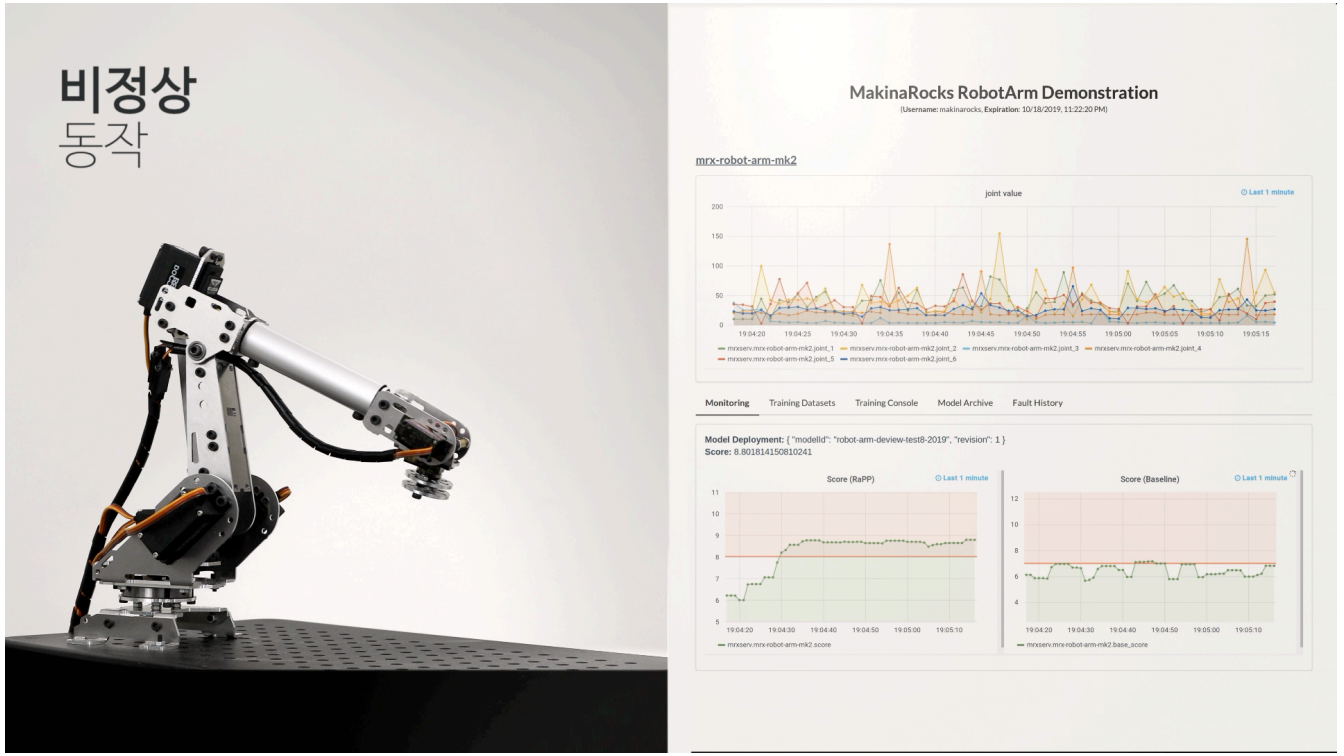


Data	AE Recon	AE RaPP	VAE Recon	VAE RaPP	AAE Recon	AAE RaPP
			Multimodal Normality			
STL	0.596	**0.714**	0.533	**0.703**	**0.716**	0.711
OTTO	0.620	**0.662**	0.598	**0.620**	0.620	**0.668**
SNSR	0.601	**0.645**	0.601	**0.630**	**0.616**	0.606
MNIST	0.825	**0.899**	0.864	**0.927**	0.847	**0.929**
F-MNIST	0.712	**0.734**	0.710	**0.737**	0.721	**0.727**
			Unimodal Normality			
MI-F	0.694	**0.707**	0.455	**0.540**	0.663	**0.704**
MI-V	0.883	**0.913**	0.680	**0.799**	0.870	**0.882**
EOPT	**0.650**	0.627	**0.604**	0.594	0.594	**0.624**
NASA	0.662	**0.665**	0.582	**0.676**	0.719	**0.724**
RARM	0.647	**0.665**	0.655	**0.678**	0.665	**0.684**
STL	0.552	**0.845**	0.526	**0.823**	0.790	**0.798**
OTTO	0.675	**0.749**	0.626	**0.741**	0.738	**0.752**
SNSR	0.791	**0.903**	0.714	**0.902**	0.863	**0.924**
MNIST	0.972	**0.979**	0.957	**0.976**	0.972	**0.977**
F-MNIST	0.924	**0.933**	0.905	**0.934**	0.922	**0.928**

Demo – RaPP를 활용한 이상탐지

DEVIEW 2019

로봇 팔의 이상동작을 효과적으로 탐지할 수 있을까?



DEVIEW
2019

DEVIEW
2019

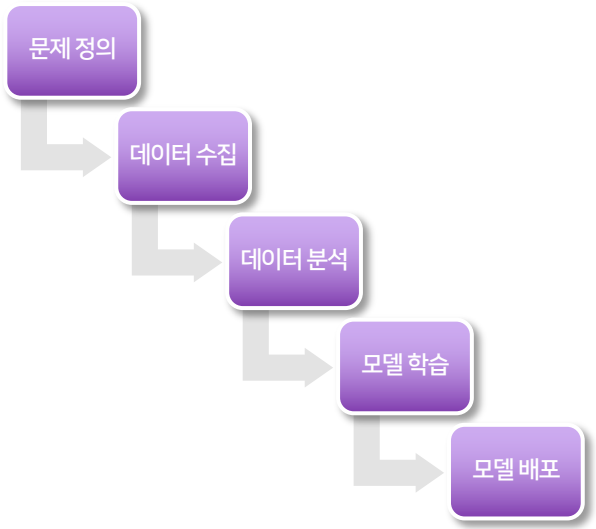
3. Beyond Deployment:

Operational AI

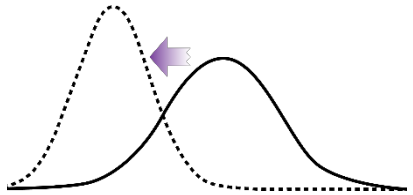
모델 학습 후 배포가 끝?

DEVIEW 2019

성능 유지 및 향상을 위한 지속적인 학습이 필요함



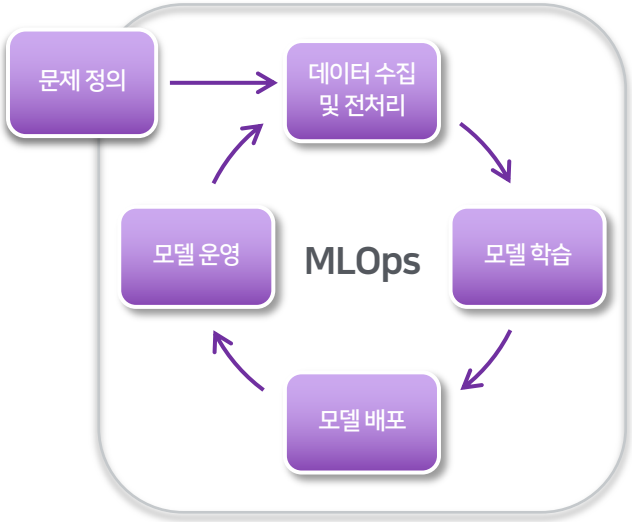
모델 학습 및 배포 파이프라인



Lifelong Learning

coner case 발생

성능 하락 발생

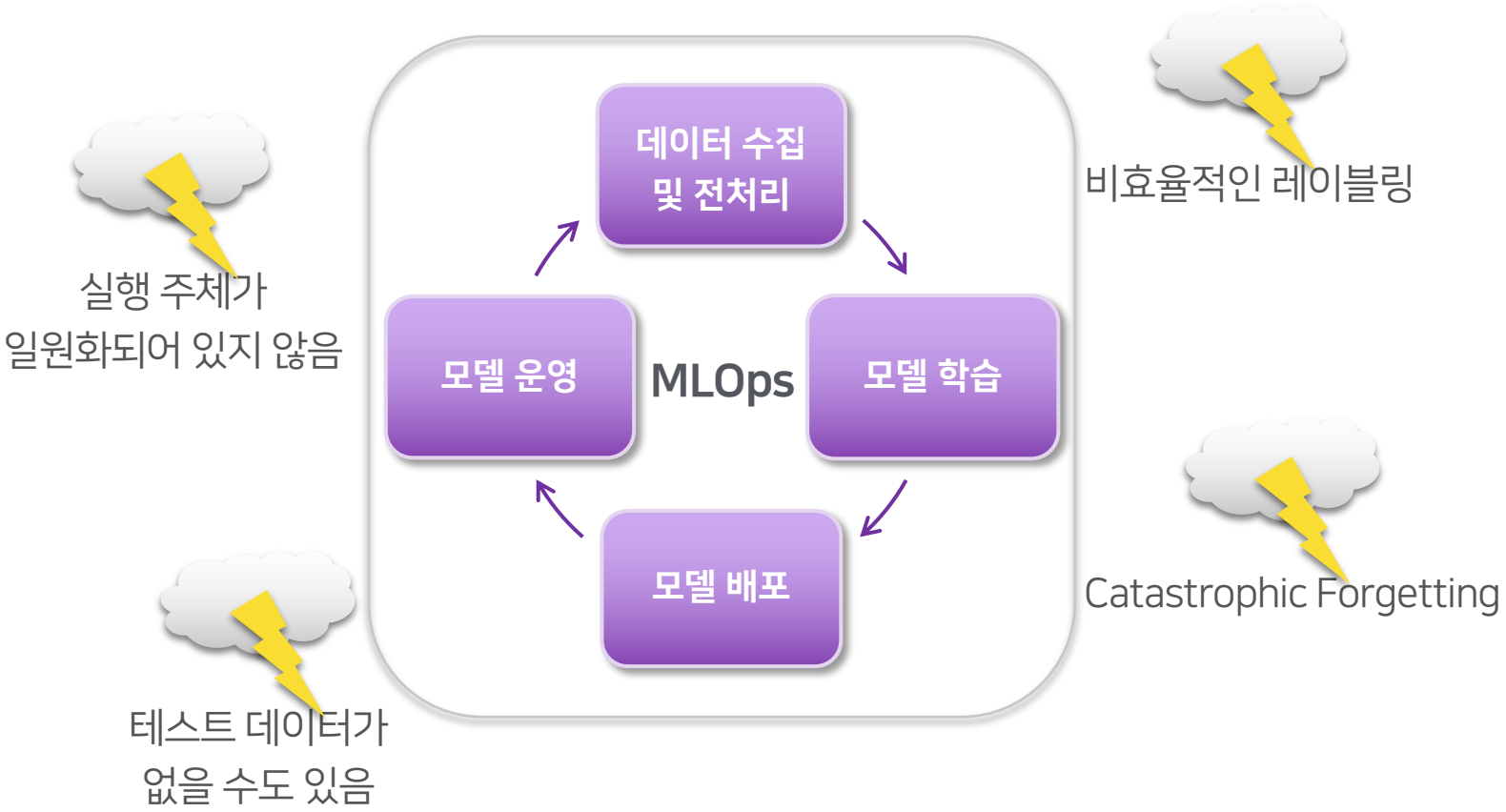


실행/운영 측면이 고려된
모델 (재)학습 및 (재)배포 파이프라인

Challenges in Lifelong Learning

DEVIEW 2019

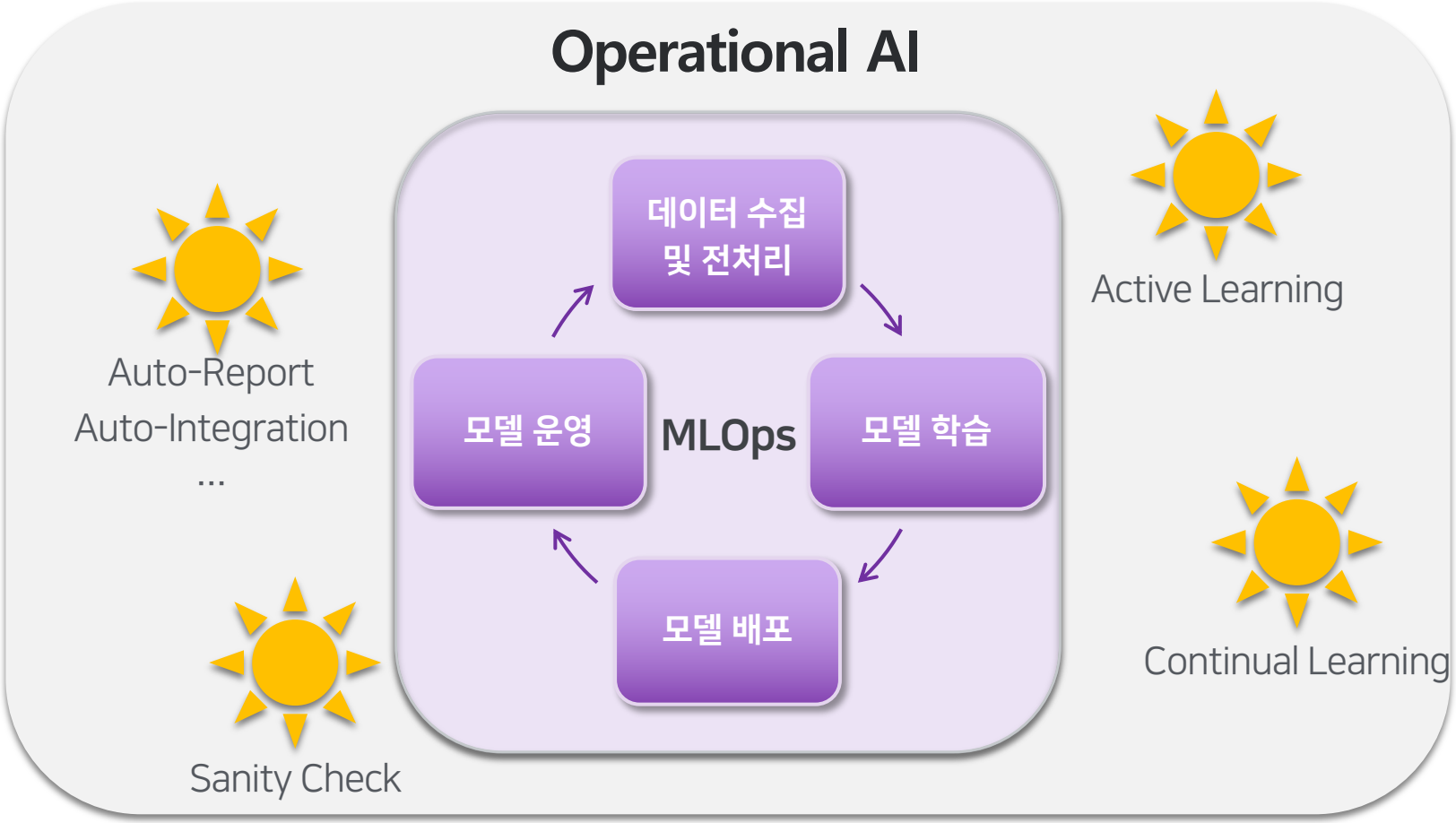
AI를 real world로 가져오기 위해선 실행/운영 측면의 문제들이 있음



Operational AI for Lifelong Learning

DEVIEW 2019

실행/운영 측면의 문제들을 해결하기 위한 AI 기술

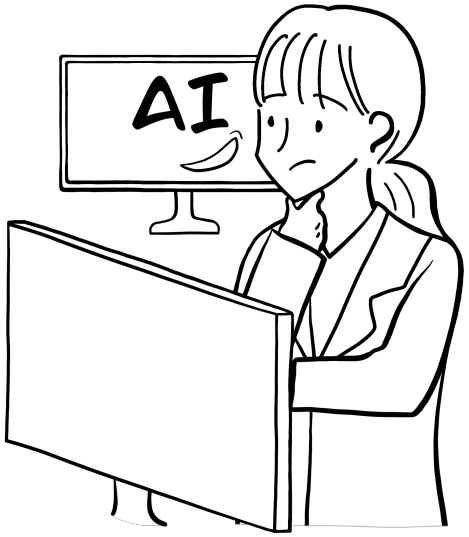


Challenges: No Test Set

실전에는 테스트 데이터가 없을 수도 있음

배포 단계

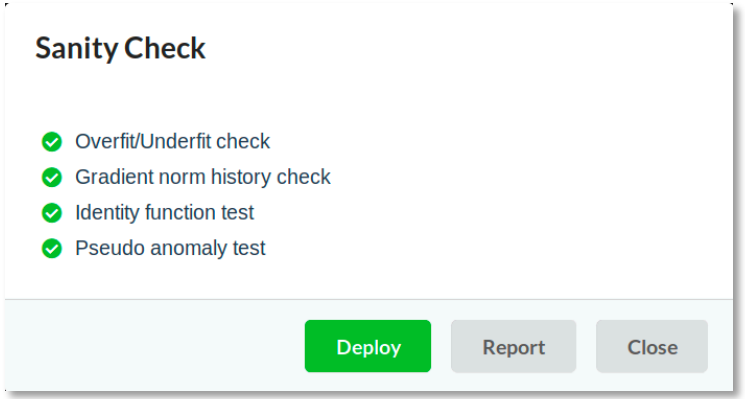
모델 성능 평가가 어려움



운영 단계

모델 성능 모니터링이 어려움

Various Sanity Checks

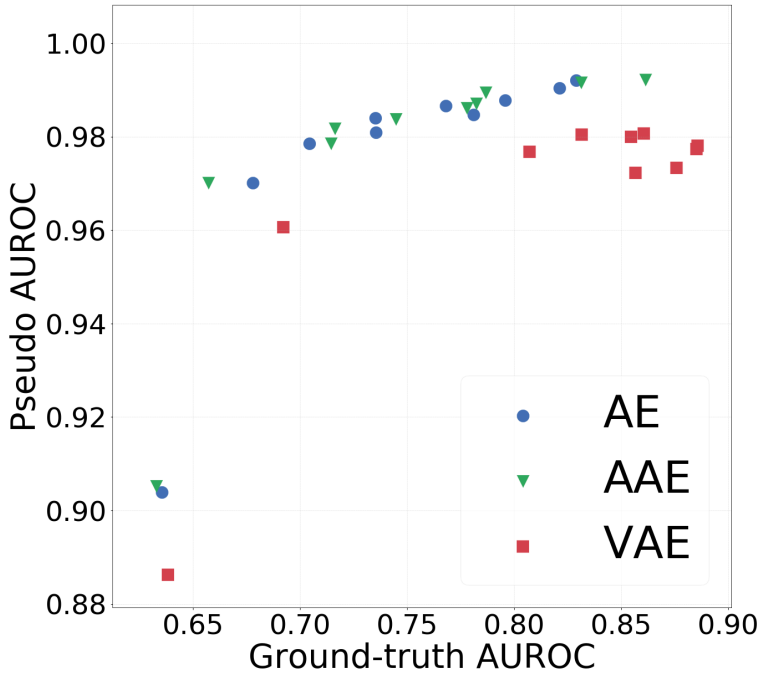


Sanity Check: Pseudo Test Set

Synthetic Anomalous를 통해 성능에 대한 Proxy를 구함

Pseudo Anomalous on MNIST

Correlation between
Ground-truth AUROC & Pseudo AUROC



Challenges: Who runs the system?

AI 개발 주체와 운영자(사용자) 주체가 다름

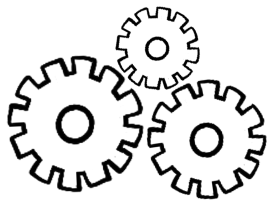
데이터 사이언티스트

(분석/AI 전문가)

- 데이터 분석/전처리
- 모델 개발/훈련/평가
- 모델 배포/통합

- Auto Model Degradation Checking
- Auto EDA / Preprocessing
- Auto Re-training
- Auto Report Generator
- Auto Integration

...



Maximized Automation for MLOps

필드 엔지니어

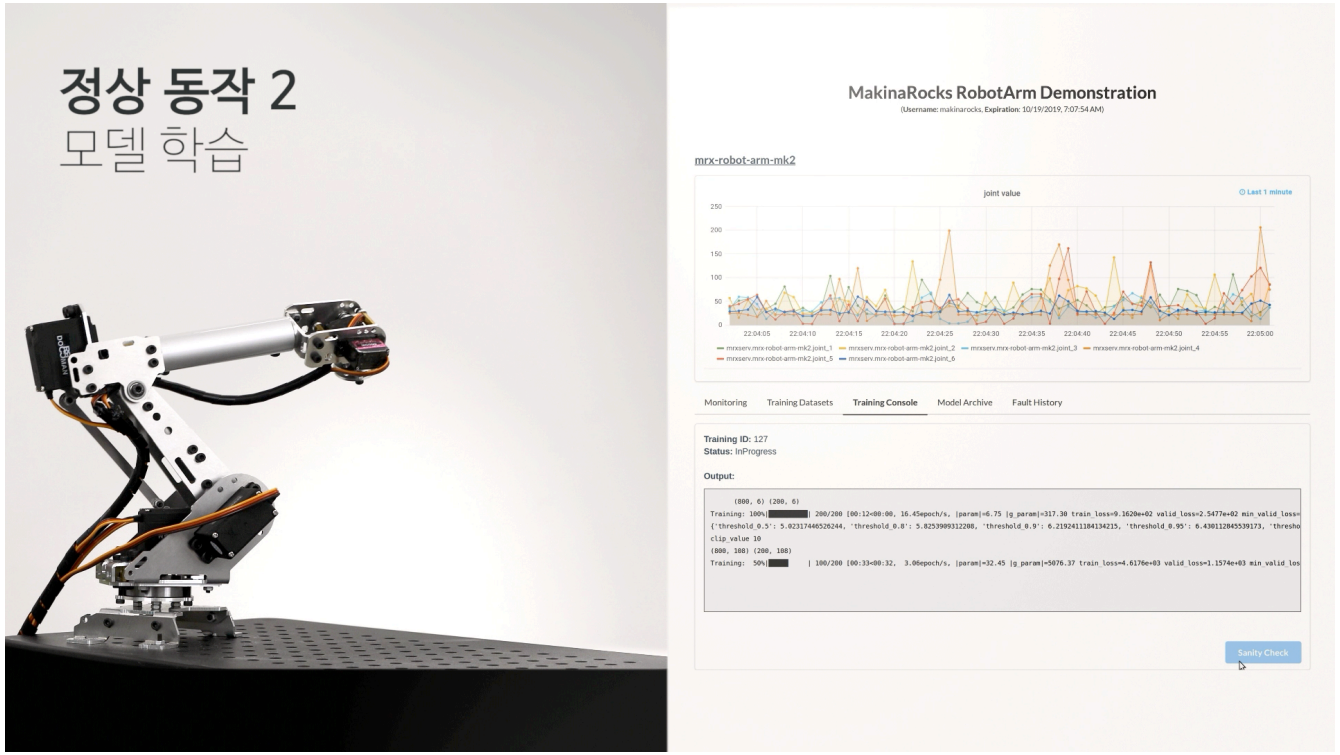
(도메인 전문가)

- 데이터 수집/레이블링
- 모델 예측 결과 모니터링
- 오작동 보고/전달

Demo – Model Update & Deploy

DEVIEW 2019

모델 배포 효율화 및 Sanity Check을 통한 모델 검증



DEVIEW
2019

Continual Learning

옛 지식을 잊지 않으면서 새로운 지식을 학습하는 AI

- **Incremental Training : 새로운 데이터만을 사용, 기존 모델 재학습**

  이전 데이터로부터 학습한 내용을 잊어버리는 현상인

  Catastrophic Forgetting이 발생함

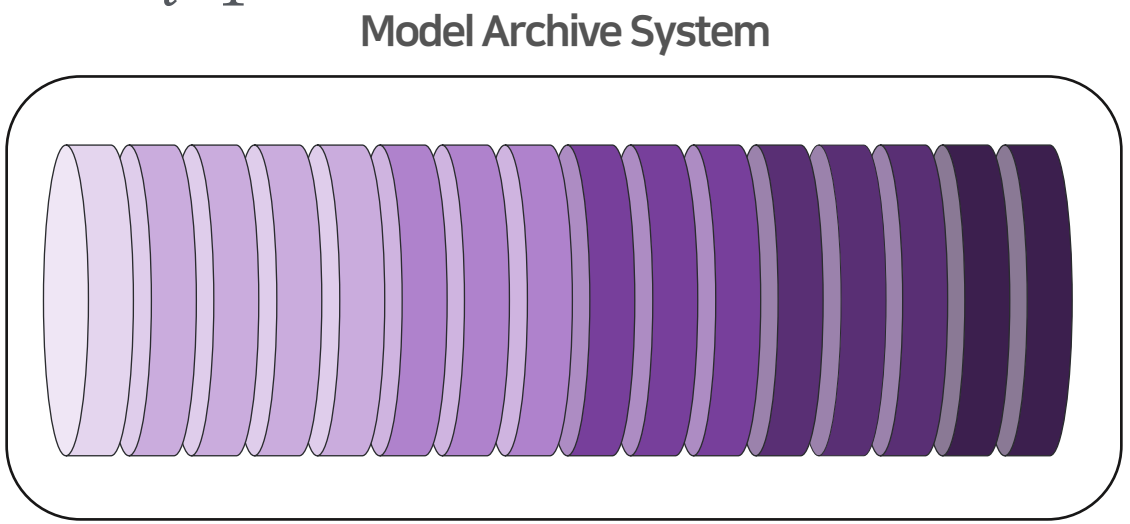
- **Inclusive Training : 전체 데이터를 사용하여 모델을 새롭게 학습**

  전체 데이터에 대한 학습은 Scalability Issue가 있음

Model Archiving

데이터에 따른 여러 모델을 만들어 문제 해결을 시도

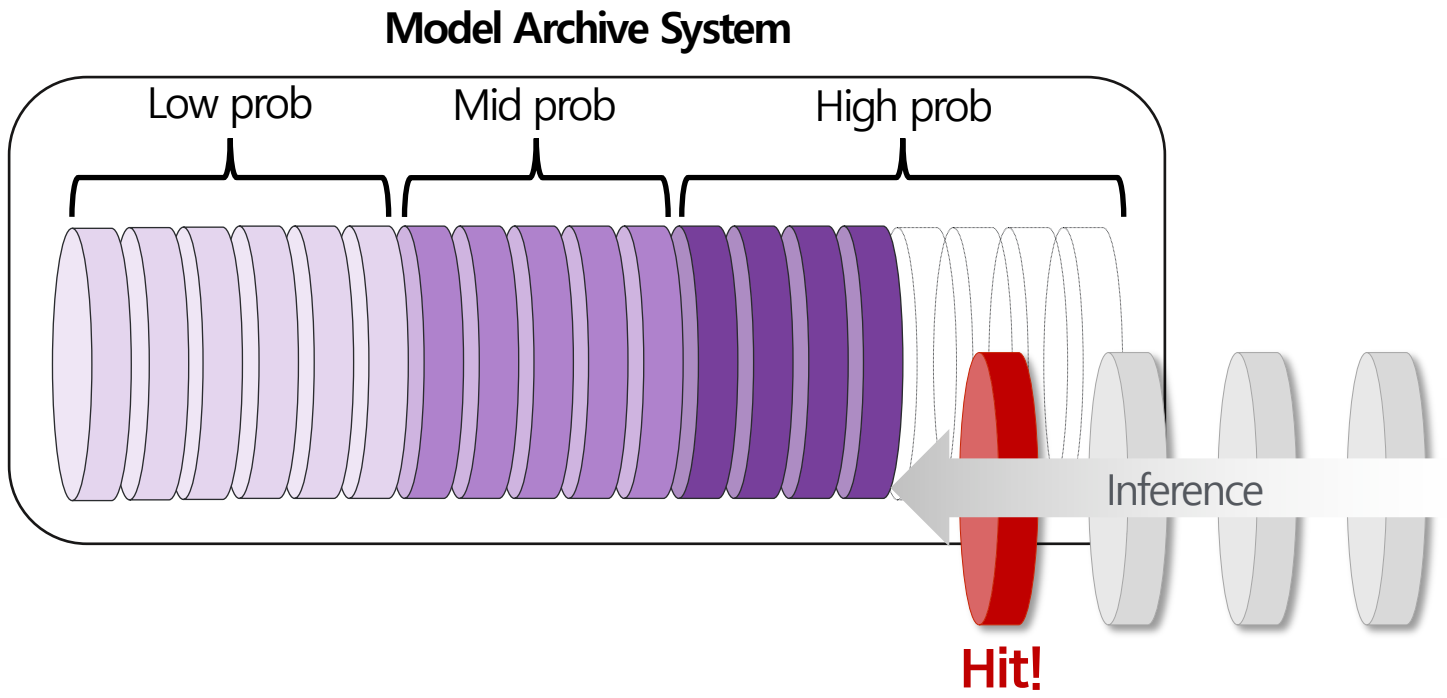
$$\text{is\_anomalous} = \prod_{i=1}^{N} f(s_i, \tau_i)\,, \text{ where } f(x, \tau) = \begin{cases} 0 & \text{if } x < \tau \\ 1 & \text{otherwise} \end{cases}.$$



Effective Model Archiving

DEVIEW 2019

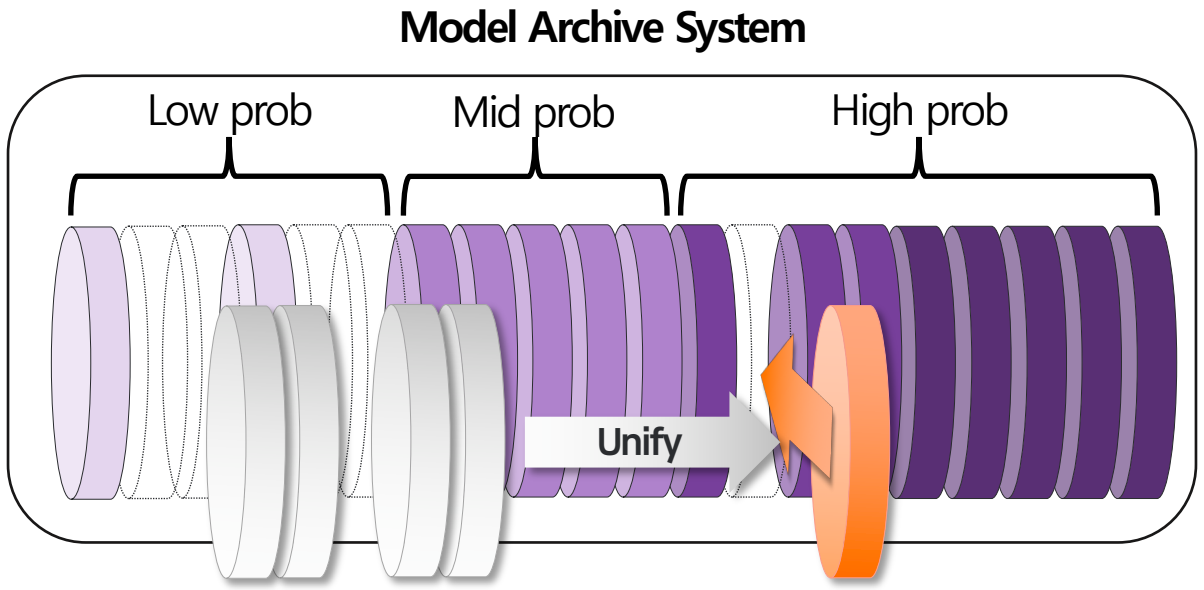
샘플이 모델에 속할 가능성을 예측하여, 불필요한 추론 과정 최소화



Effective Model Archiving

DEVIEW 2019

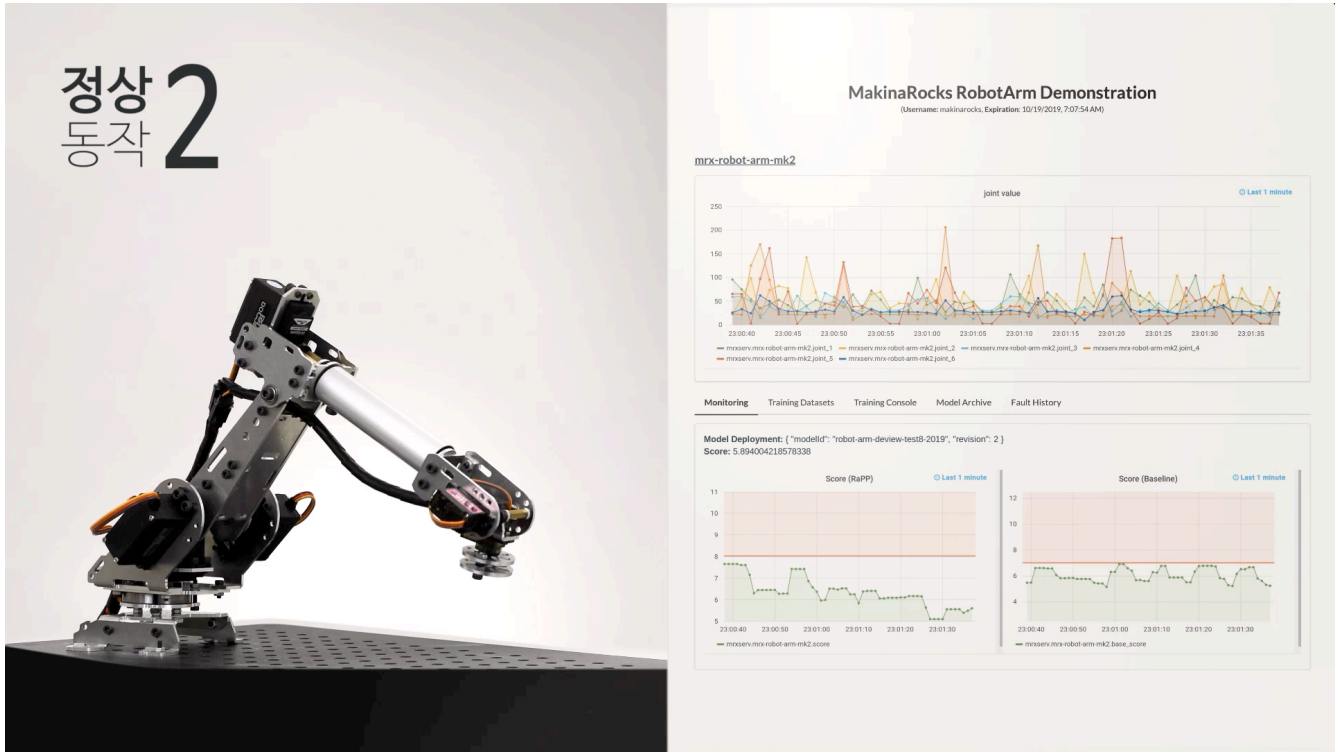
비슷한 분포를 위한 모델들을 재학습하여 통합 및 성능 향상



Demo – Model Archiving

DEVIEW 2019

전체 데이터에 대한 재학습 없이 새로운 데이터에 대처 가능



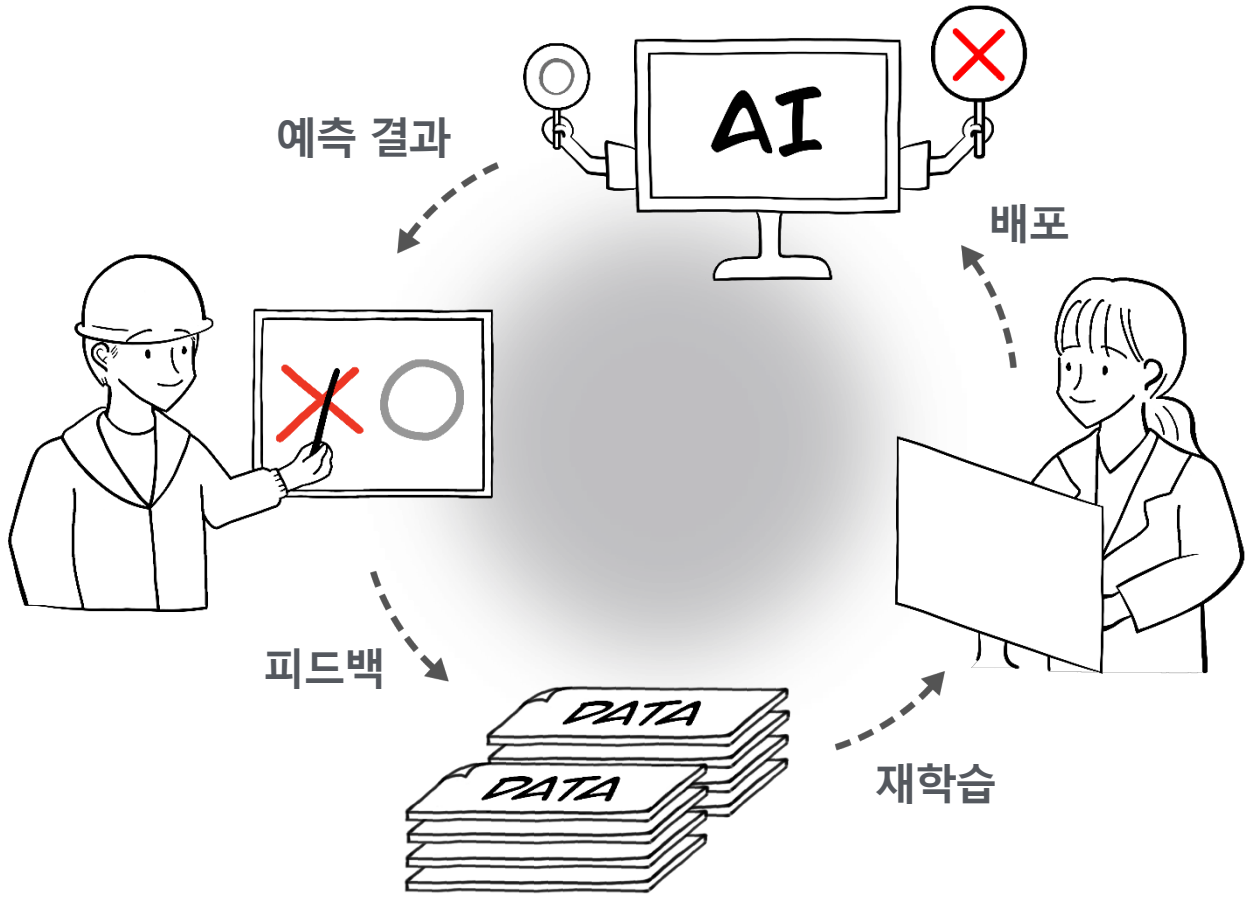
DEVIEW
2019

DEVIEW
2019

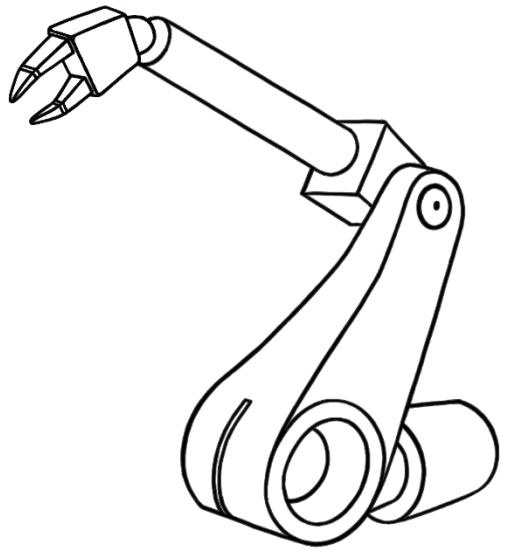
4. AI in the Loop?

Current: Human in the Loop

인간의 피드백을 통해 성장하는 AI

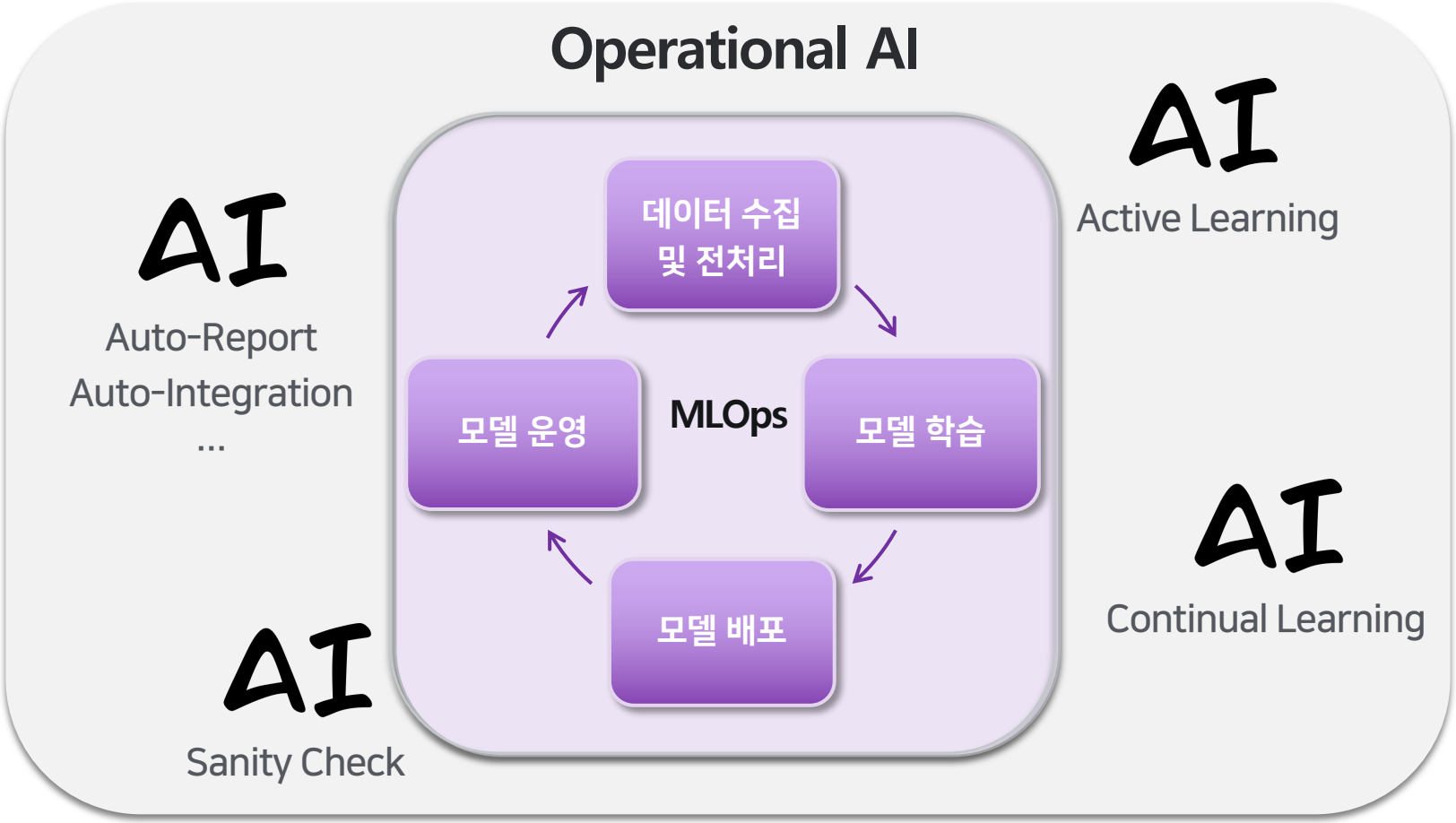


raw data



Future: AI in the Loop

AI driven Lifelong Learning



DEVIEW 2019

Q & A

DEVIEW
2019

Thank You