4차 산업 혁명과 여성과학자의 역할

2017년 한국정보보호학회 하계학술대회

정윤경
성균관대학교 소프트웨어대학

성균관대학교
SUNG KYUN KWAN UNIVERSITY(SKKU)

4차 산업혁명에 대한 두려움과 불안

소개

성균관대 정보공학과 학/석사

LG전자 3년 근무

미국 North Carolina 주립대 Computer Science 박사 6년

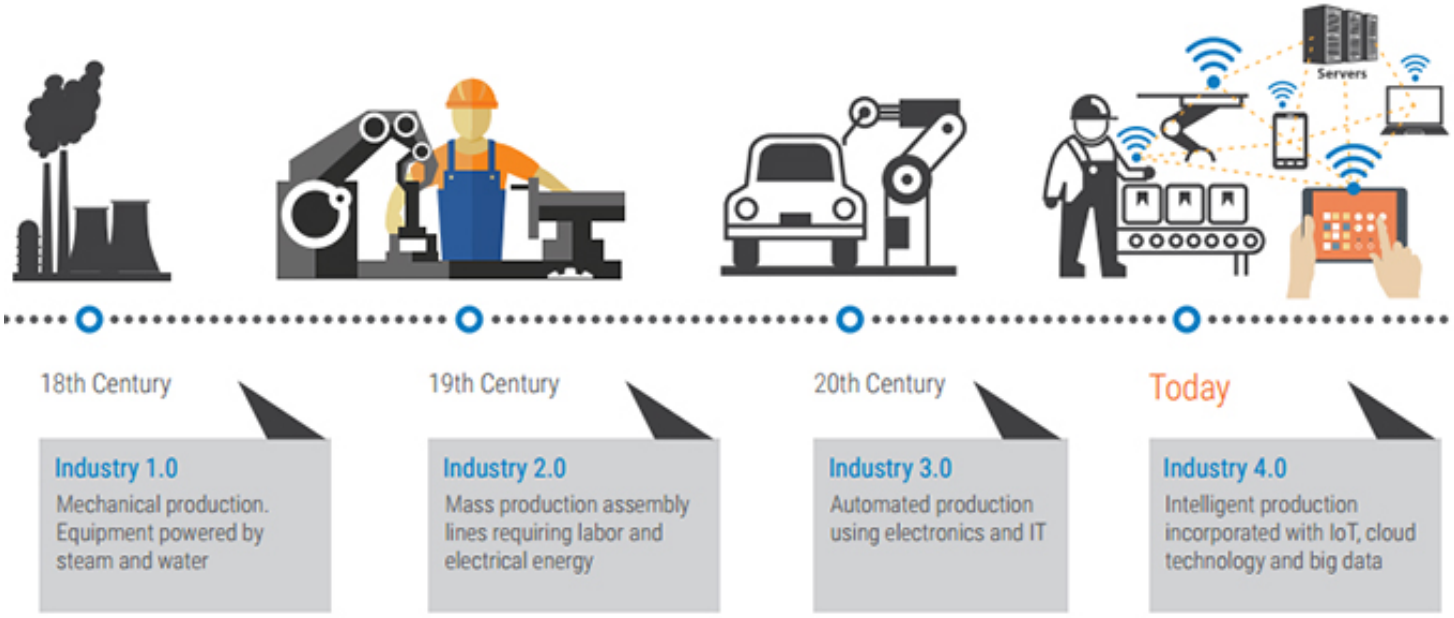
삼성전자 종합기술원 2년 6개월

덴마크 IT University of Copenhagen, 포닥 4년

성균관대 조교수 3년차

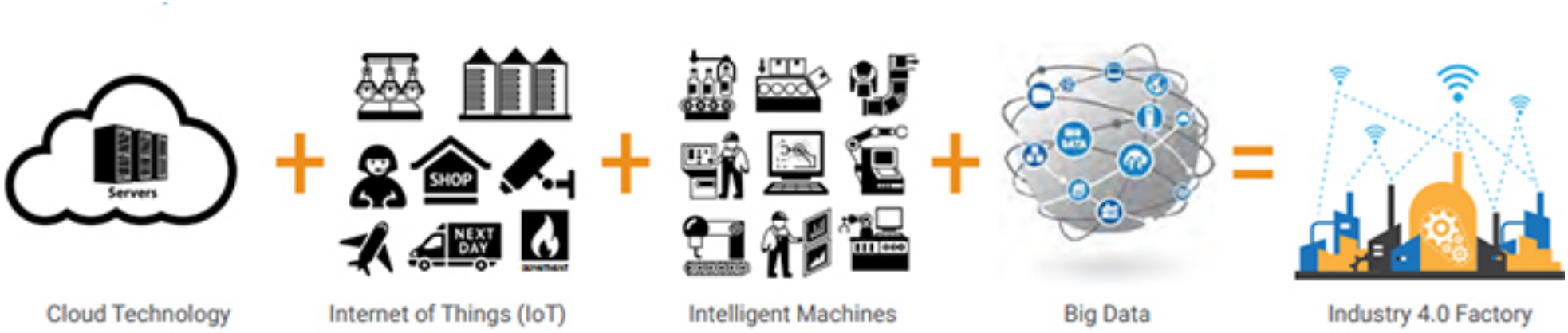
4차 산업혁명

인간의 지적 노동을 자동화 (기계의 지능화)로 인한 생산성 향상

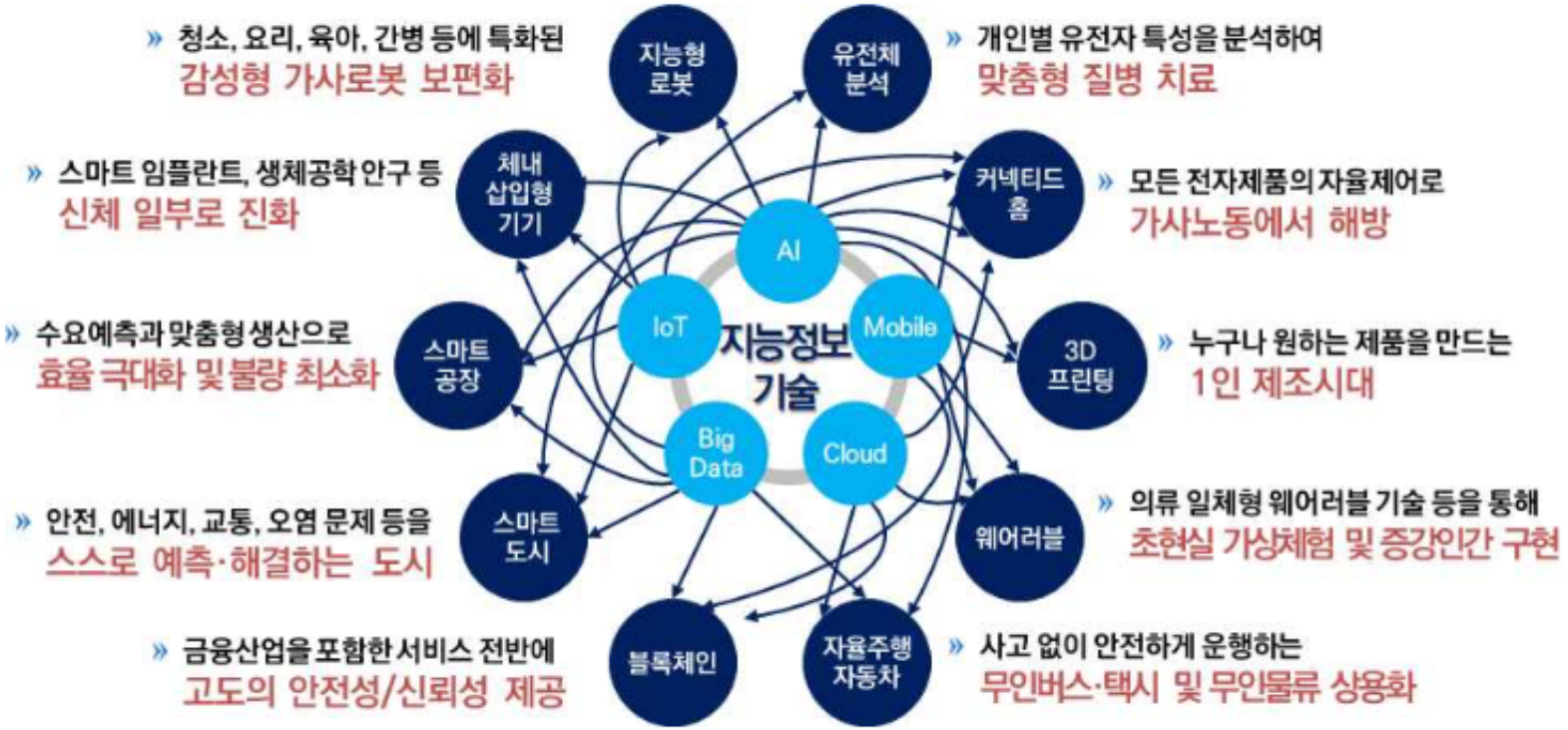


출처: BCM Advanced Research

4차 산업혁명의 핵심 기술



인공지능 기술과 타산업/기술의 융합



출처: 지능정보사회 중장기 종합대책 (2016.12)

Amazon Go

Amazon이 Whole Foods를 14조원에 인수 (2017.6.17)

Virtual Assistant (Siri, MS Cortana)

삼성전자는 2016년 하만 그룹을 8조원에 인수

4차 산업혁명을 대비하는 국가의 정책

전 산업의 지능 정보화

기계가 학습 가능한 양질의 데이터 수집, 활용 및 거

4차 산업혁명 보안 관련 국가의 정책

AI기반 제품(CCTV, 자동차, 로봇 등) 및 비정형 데이터까지 사이버 위협정보 수집 대상을 확대하고 이에 기반한 사이버보안 빅데이터센터 구축('17년~)

인공지능에 기반한 사이버 면역시스템 및 자가 방어체계 구축

- 평상시, 다양한 악성코드 및 취약점에 관한 정보를 AI가 수집 분석하여 공격 상황에 대비하는 사이버 면역시스템 개발('18년~)
- 공격 발생시, AI가 스스로 핵심 데이터 은폐 및 암호화, 전송경로 변경 등을 통해 방어력을 높이는 자율 방어체계 구축('20년~)

네트워크로 연결되는 수많은 개인용 AI기기·서비스의 보안취약점을 자동관리하는 개인 맞춤형 지능보안시스템(Personal AI Shield) 개발(~'25년)

출처: 지능정보사회 중장기 종합대책 (2016.12)

4차 산업혁명을 대비하는 국가의 정책

전 산업의 지능 정보화

기계가 학습 가능한 양질의
데이터 수집, 활용 및 거

인공지능을 배우자!

인공지능을 공부한다는 것은

기술력

기술 활용 능력

- 서비스 디자인
- 도메인 지식

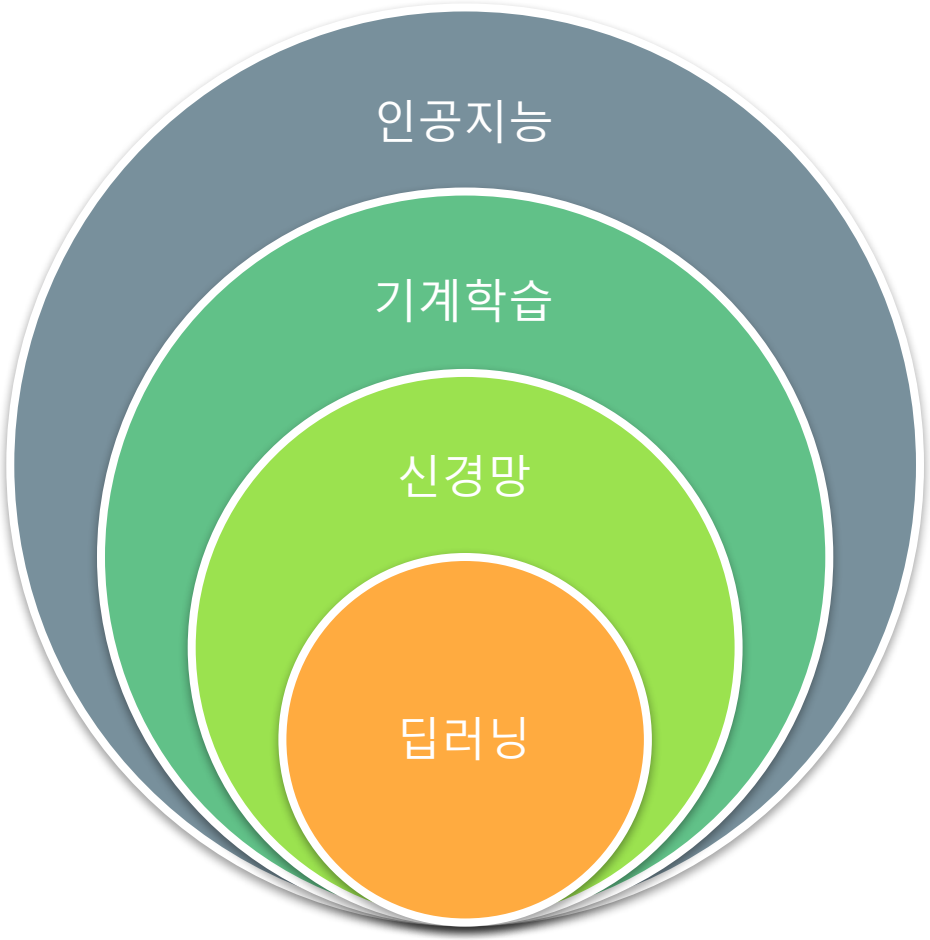
서비스 디자인

- 창의력
- 호기심
- 관찰력
- 스스로 생각하는 능력
- 사물을 다르게 보는 능력
- 실천력

- 낯선 것과 환경에 자주 노출
- 여행
- 자신만의 세계관을 정립
- 책
- 그림 그리기
- 신문, 잡지 구독
- 과감해지기, 과하게 해보기
- 통 크게 살기

보안분야에서의 AI 활용

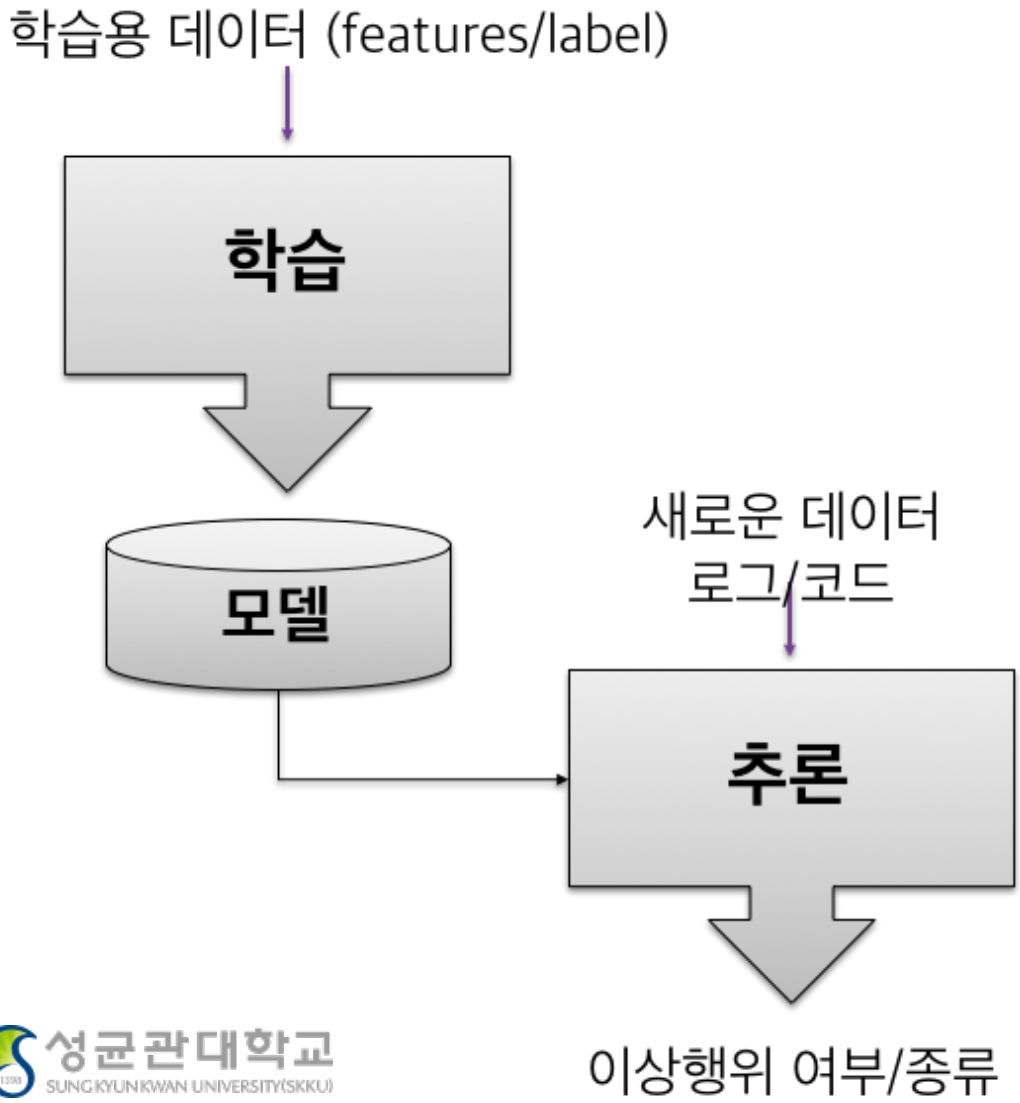
- 부정사용 방지 시스템
  - 전자금융거래에 사용되는 단말기 정보, 거래내용 등을 종합적으로 분석하여 의심 거래를 탐지하고 차단
  - 딥러닝이 적용된 FDS에서는 기계 스스로 정상 거래 패턴과 부정 거래 패턴을 분석·학습해 이상 거래 여부를 판별
- 이상행위 탐지 (UBA: User Behavior Analysis)
  - 개인과 조직의 프로파일 정보를 축적하는 '프로파일링' 기법 사용.
  - 개인의 행동에서 보안을 위해하는 score가 임계치 이상이 되는 경우 이상으로 판단. 임계치를 설정하는 부분을 ML 기술로 학습하여 해결
- 암호화


인공지능
기계학습
신경망
딥러닝

기계 학습

기계 학습 (Machine Learning)

- 기계 학습 알고리즘이 하는 일은 몇 개의 범주 (category)로 데이터가 분류되어 있을 때, 주어진 데이터를 해당 클래스에 맞도록 분류할 수 있는 기준 (분류기)을 찾는 기술
- 기계 학습은 학습 + 추론(분류) 을 수행
- 활용: 스팸 이메일 필터링, 신용카드 비정상적 거래, 음성 인식, 필기체 인식, 정보 검색, 오피니언 마이닝 등 패턴 인식이 문제 해결에 핵심인 분야



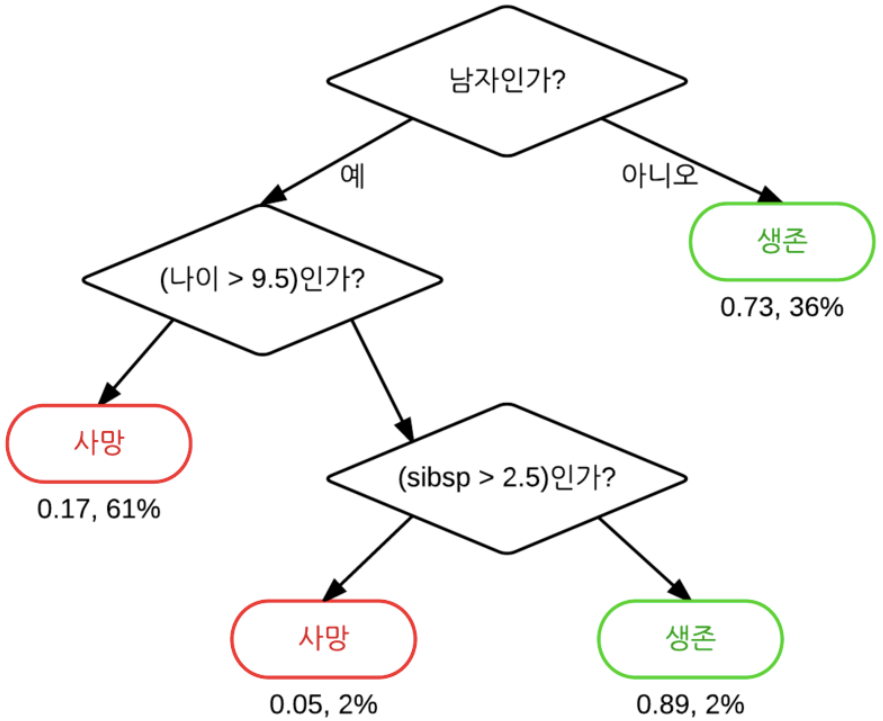

```
Aug 25 09:10:01 localhost CROND[5442]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 09:20:01 localhost CROND[5474]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 09:30:01 localhost CROND[5503]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 09:40:01 localhost CROND[5544]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 09:50:02 localhost CROND[5580]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 10:00:01 localhost CROND[5623]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 10:01:01 localhost CROND[5629]: (root) CMD (run-parts /etc/cron.hourly)
Aug 25 10:01:01 localhost run-parts(/etc/cron.hourly)[5629]: starting 0anacron
Aug 25 10:01:01 localhost run-parts(/etc/cron.hourly)[5638]: finished 0anacron
Aug 25 10:10:01 localhost CROND[5738]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 10:20:01 localhost CROND[5868]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 10:30:01 localhost CROND[6170]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 10:40:01 localhost CROND[6326]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 10:50:01 localhost CROND[6388]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 11:00:01 localhost CROND[6419]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 11:01:01 localhost CROND[6425]: (root) CMD (run-parts /etc/cron.hourly)
Aug 25 11:01:01 localhost run-parts(/etc/cron.hourly)[6425]: starting 0anacron
Aug 25 11:01:01 localhost run-parts(/etc/cron.hourly)[6434]: finished 0anacron
Aug 25 11:10:01 localhost CROND[6465]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 11:20:01 localhost CROND[6560]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 11:30:02 localhost CROND[6642]: (root) CMD (/usr/lib/sa/sa1 1 1)
Aug 25 11:40:01 localhost CROND[6723]: (root) CMD (/usr/lib/sa/sa1 1 1)
```

학습용 데이터

학습 알고리즘	설명
결정트리	특정 사례가 어떤 클래스에 속하는지 분류하는 과정을 트리의 형태로 표현. 훈련 데이터가 주어지면 트리를 자동으로 생성. 유일하게 학습 과정의 지식을 도출할 수 있는 알고리즘
SVM	다차원 공간에서 서로 다른 클래스를 분류하는 support vector를 주어진 데이터로부터 결정하는 알고리즘. 가장 효율이 높은 것으로 알려짐.
K-means clustering	다차원 공간에서 특정 사례를 표현했을때, 입력된 사례와 가장 가까운 mean값이 해당하는 클래스로 예측
베이지안 네트워크	지식과 추론을 조건부 확률 네트워크로 표현
신경망	이진 결과를 출력하는 노드의 집합으로 입력과 출력 정보를 표현하고, 입력층과 출력층간 연결을 담당하는 은닉층으로 설계된 네트워크 구조

결정트리 (Decision Tree)

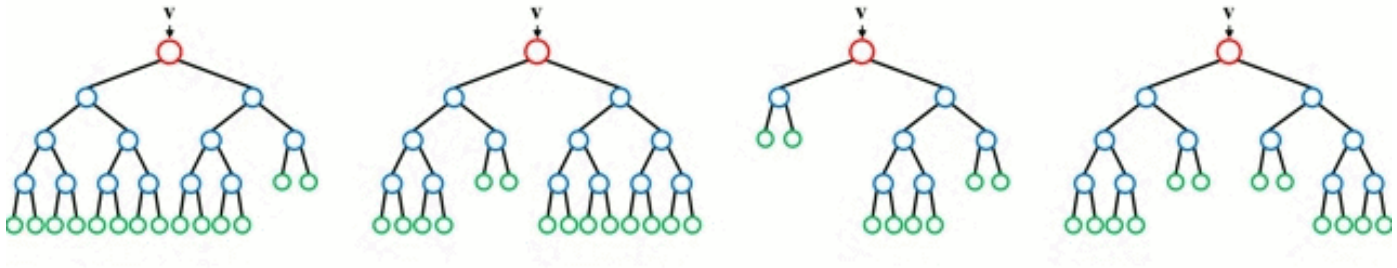
- 각 노드는 속성을 의미
- Branch마다 속성에 대한 값
- Information Gain이 최대가 되도록 자식 노드를 생성



타이타닉호 탑승객의 생존 여부를 나타내는 결정 트리. (“sibsp”는 탑승한 배우자와 자녀의 수를 의미한다.) 잎 아래의 숫자는 각각 생존 확률과 탑승객이 그 잎에 해당될 확률을 의미

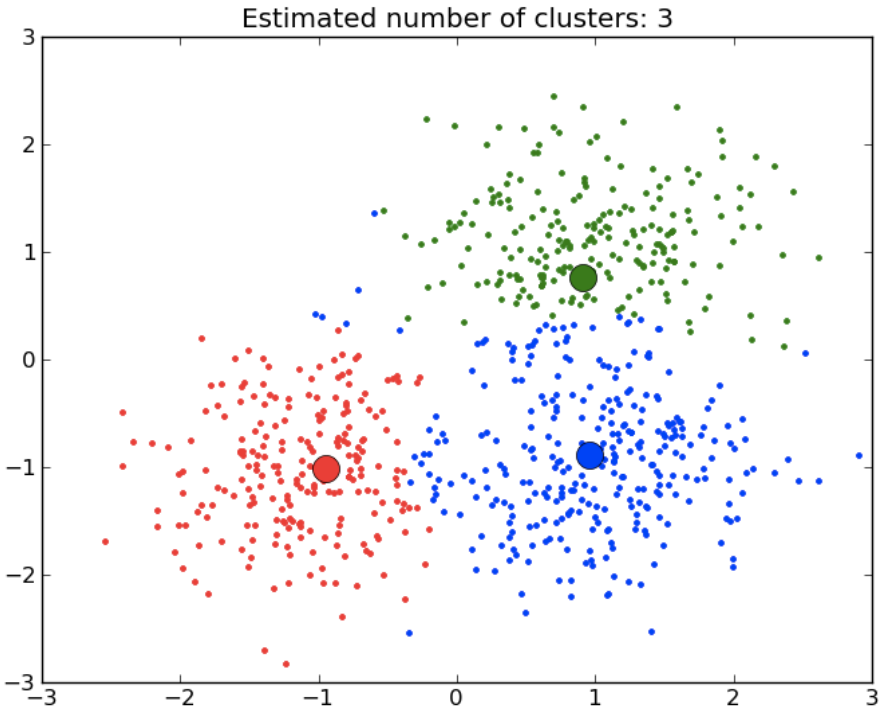
Random Forest

- 훈련 데이터를 분할하여 여러 트리를 학습
- 주어진 데이터의 결과를 평균 혹은 투표로 결정



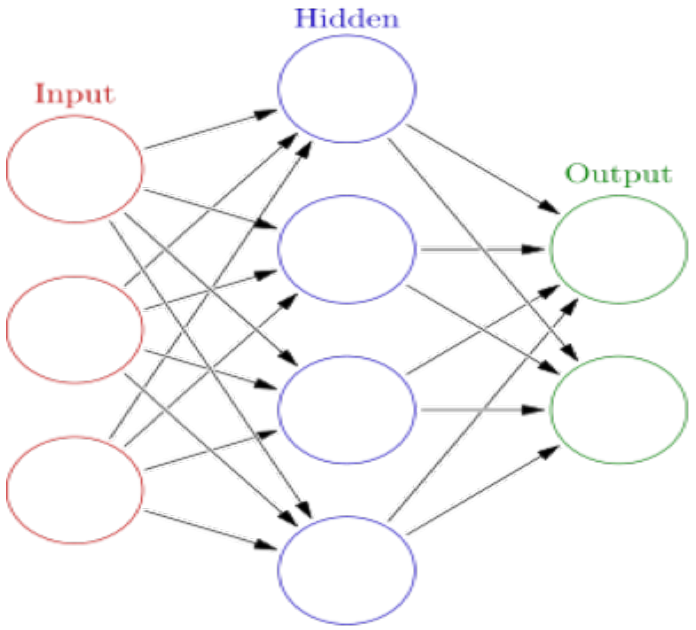
비지도 학습 - clustering

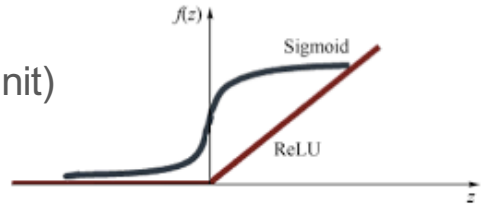
- 터에서 label 정보가 없음
- 새로운 종류의 공격을 탐지하는 데에 활용
- Clustering algorithm
- K-means algorithm



신경망(Artificial Neural Network)

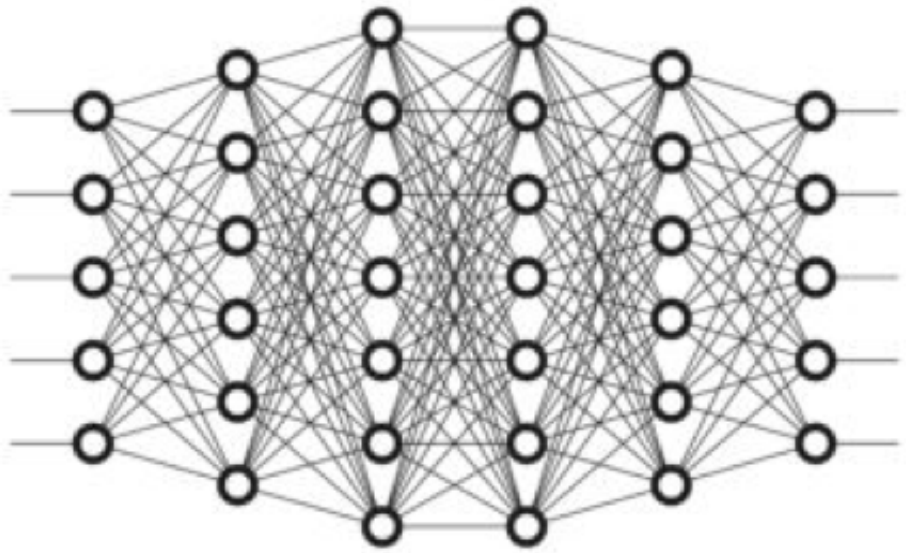
- 사람의 뉴런 동작 방식을 모사
- 노드는 입력받은 신호의 가중치가 반영된 총합을 구하고, 그 합이 임계치 이상인 경우 1을, 아닌 경우 0을 출력. 1을 출력하는 것을 활성화(activation)
- 입력/은닉/출력층 노드간의 연결 강도를 나타내는 가중치를 최종 출력 결과가 좋도록 최적 값을 찾는 것이 학습
- 활성화 함수
- Sigmoid / ReLU(Rectified Linear Unit)





Deep Learning

- 신경망의 은닉층수를 높인 확장된 기술
- 기존 단일 컴퓨터의 파워로 계산할 수 없던 것이 GPU를 병렬 활용과 학습을 위한 데이터가 풍부해지면서 가능해짐
- 특징 선택이 자동화 되면서 문제 도메인에 대한 비전문가도 신경망을 이용하여 문제를 풀 수 있게 됨



딥러닝 기술	설명
DNN (deep neural network)	은닉층이 깊고 속성 선택 단계가 없는 신경망 구조
CNN (convolutional neural network)	입력의 차원 정보를 유지하는 딥러닝 네트워크 구조로 주로 이미지 인식에 활용
RNN (recurrent neural network)	은닉층이 과거의 상태를 저장하여 시퀀스 및 시계열 데이터에 활용되는 딥러닝 네트워크 구조
LSTM(Long Short Term Memory)	오래된 과거의 정보를 저장할 수 있는 구조
Autoencoder	입력 정보와 동일한 정보를 출력하는 단일 은닉층 신경망 구조. 즉, 입력을 복원하는 기능을 수행
GANs(Generative Adversarial Networks)	주어진 훈련 데이터에서 유사한 가짜 데이터를 만들어 내는 생성기와, 진짜 데이터와 가짜 데이터를 식별하는 분류기를 학습

요약

- 4차 산업혁명은 위기와 기회
- 인공지능 기술 활용력이 중요
- 보안 분야에서는 비지도 학습, 베이지언 추론, 신경망, 딥러닝 기술을 활용하여 자동화하고 관리자가 확인하는 human-assisted AI 형태로 인공지능을 활용
- 신경망, 딥러닝 기술

여성 과학자로서의 당부

SW 분야의 전문가라는 점에서 이미 인재

여성답다라는 말에 현혹되지 말고

나와 타인의 단점을 인정하며

자기 자신이 행복해지는 방향으로 나아가세요.

성균관대학교 소프트웨어대학
정윤경
aimecca@skku.edu

성균관대학교
SUNG KYUN KWAN UNIVERSITY(SKKU)