2021-06-14

이상의 종류>

1) 점 이상(point anomaly)

자료 내 하나의 개체가 나머지에 대해 이상하다고 판단되는 경우

2) 맥락적 이상(contextual anomaly)

자료 내 개체가 특정 맥락에서 이상하다고 판단되는 경우

이상 여부는 특정한 맥락에서 행동 변수(맥락적이지 않은 수치적인 특성)의 값으로 판단한다.

Ex) 겨울에 기온이 1.7도인 것은 그럴 만하지만, 여름에는 매우 이상한 상황이다.

supervised anomaly detection

일반적인 예측 모델을 세우는 과정과 비슷함

semi-supervised anomaly detection

일반적으로 정상 자료만을 사용하여 모델을 학습시킨 뒤 시험 자료에 적용하는 방식을 이용

unsupervised anomaly detection

가장 널리 쓰일 수 있음, 주로 자료 내 개체들 간의 거리를 기반으로 해서 이상값을 탐지한다.

연구 분야별 이상 탐지 기법 활용 사례>

침입 탐지) 대용량의 자료를 다루기 위해 효율적인 계산이 필요하며, 오경보율(false alarm rate)이 조금만 높아져도 분석에 큰 부담이 될 수 있다. 오경보율이란 이상값이라고 예측했는데 그것이 틀린 예측인 것들의 비율이다. 또한 자료가 순간마다 생겨나기 때문에 실시간 분석이 요구된다.

Ex) 국내 대표적인 보안관제 전문기업인 이글루시큐리티는 지난 2018년 1월 대구 AI 기반 지능형 보안관제 체계(D-Security) 구축을 완료했다. AI 시스템은 대구시의 정보자산 시스템에 대해 악의적인 사이버 위협을 가하는 공격자의 특성이 담긴 데이터를 학습하여 이상 탐지 알고리즘에 적 용한다.

시만텍(Symantec)은 실시간으로 외부 공격자로부터 보안 위협 및 이상 징후를 탐지하여 차량의 보안 상태를 실시간으로 알려 주는 수동 침입 탐지 보안 소프트웨어를 개발한 바 있다.