

제목 : 산업 제어 시스템의 이상 탐지 모델에 대한 적대적 예제 공격 및 대응

1. 논문 핵심 요약

산업 제어 시스템에서의 이상 징후 탐지 모델에 대한 적대적 예제 공격과 이에 대한 대응 방안 다룸.

2. 주요 내용 -개발

이상 징후 탐지는 스마트 공장과 같은 산업 제어 시스템에서 중요한 보안 측면이며, 딥러닝 기법과 설명 가능한 인공지능(XAI) 기술을 활용하여 이를 탐지하는 모델을 개발

3. 주요 내용 -운영

설명 가능한 인공지능 기술을 적용하여 보안 담당자에게 이상 징후에 기여한 센서를 제시하여 실질적인 조치와 운영을 지원