인공지능(AI) 기술을 적용한 지방자치단체의 물리적 보안 개선방안

Measures to Improve Physical Security of Local Governments Using Artificial Intelligence (AI) Technology

정 우 석* · 김 태 환**

Jeong, Woo_Seok · Kim, Tae_Hwan

요 약

인공지능(AI)은 지방자치단체 청사의 물리적 보안 시스템을 개선하는 데 활용될 수 있는 유망한 기술이다. 방대한 데이터를 분석하고 패턴을 식별할 수 있어, 테러나 폭력과 같은 위협을 사전에 예방하는데 도움이 될 수 있다. 또한, 인공지능(AI)은 실시간으로 보안 상황을 모니터링하고 이상 징후를 감지할 수 있어, 보안 인력의 업무 효율성을 향상시키고 비용을 절감하는 데에도 도움이 되기에 인공지능(AI)을 적용한 물리적 보안 시스템 개선방안에 대해 제안하고자 한다.

Keywords : 인공지능(AI), 지방자치단체 , 청사방호, 물리적 보안, 사이버 보안

1. 서 론

지방자치단체 청사는 지방정부의 업무를 수행하고 시민에게 행정서비스를 제공한다. 따라서 안전하게 보호되어야 하며, 물리적 보안은 지방자치단체의 중요한 업무 중 하나이다. 물리적 보안의 목적은 테러, 폭력, 재난과 같은 위협으로부터 청사와 시설을 보호하고 청사에 출입하는 사람과 직원을 보호하는 것이다. 최근에는 테러, 사이버 공격과 같은 새로운 위협이 등장하고 있어 이에 대응하기 위한 물리적 보안체계가 중요하다. 이를 위해서는 보안 인력의 전문성 향상과 장비의 최신화가 필요함에 따라 인공지능(AI)은 물리적 보안을 개선하는데 사용할 수 있는 유망한 기술이다. 인공지능(AI)은 방대한 데이터를 분석하고 패턴을 식별하여 테러나 폭력과 같은 위협을 사전에 예방하는 데 도움이 될 뿐만 아니라 실시간으로 보안 상황을 모니터링하고 이상 징후를 감지하는데 사용할 수 있다.

2. 인공지능(AI)을 적용한 물리적 보안 이점

2.1 사전 예방 및 오프라인 위험 대응

보안 인공지능은 오프라인에서 벌어질 수 있는 더 많은 위험에 대응할 수 있다. 예를 들어 CCTV 영상을 모니터링 하거나 경보에 대응하는 등 현재 보안 요원이 수행하는 많은 작업을 자동화 하는 곳에 사용할 수 있으며, 범죄가 발생할 가능성이 있는 장소와 시간 등 잠재적인 위험을 예측하여 정보를 주기도 하고 비즈니스의 특정 요구사항에 맞게 보안 경고를 맞춤 설정하거나, 개인의 위험 프로필에 맞는 보안 조치를 추천 받을 수 있다.

2.2 사이버 보안 위협 대응

오프라인의 위험 뿐만 아니라 사이버 공간에서의 위협도 많은 문제점으로 대두되고 있다. 수없이 많은 사이버 보안 위험 사례를 처리하기 위해서는 많은 인력이 필요하지만 보안 툴에 AI를 적용하여 확장 가능한 솔루션을 구축하면, 이러한 문제점을 극복할 수 있다. 또한, 위험 자동 탐지나 위험에 대한 자동 대응, 소프트웨어 패치 또는 업데이트 등의 반복적인 작업을 자동화하면 인간의 작업 시간을 축소할 수 있을 뿐만 아니라 AI는 대량의 데이터를 실시간 분석하는 데에 특화되어 있기 때문에, 이를 기반으로 인간 분석가보다 더 빠르고 정확하게 잠재적인 위험을 식별할 수 있다.

* 정회원 · 용인대학교 대학원 경호학과 박사과정 hwarang287@hanmail.net

** 정회원 · 용인대학교 경호학과 교수 kosdi1004@hanmail.net

3. 인공지능(AI)을 적용한 물리적 보안의 한계

3.1 기술적인 한계

보안 인공지능(AI)은 많은 장점과 혁신적인 기회를 제공하지만 기술적인 한계도 여전히 가지고 있다. 인공지능(AI) 모델은 훈련을 위해 대규모 데이터 세트에 크게 의존하므로 만약 학습자가 악의적인 의도를 가지고 있거나, 조작된 데이터를 주입할 수 있다면 AI 시스템의 성능과 동작에 영향을 미칠뿐만 아니라 이로 인해 편향되거나 부정확한 결과가 발생하여, 시스템이 취약해지거나 신뢰할 수 없게 된다. 또한, 인공지능(AI) 시스템은 편견을 포함하거나 사회적 편견을 반영할 수 있는 과거의 데이터를 기반으로 훈련이 되기 때문에 편견이 적절하게 해결되지 않으면, 차별이나 불공정한 관행이 지속되어 사회적, 윤리적 문제를 야기할 수 있다.

3.2 인공지능(AI)의 발전과 맞물린 보안 취약 문제

인공지능(AI) 기술의 발전은 보안 업계에 양날의 검으로 작용하는데 특히, Chat GPT와 같은 Generative AI 분야에서 그 영향이 두드러지게 나타난다. Chat GPT는 보안 취약점을 찾거나 해킹에 활용할 수 있는 소스 코드를 생성하는 등 악용될 수 있는 가능성을 가지고 있으며, Chat GPT와 같은 Generative AI 모델은 직접적인 악성 코드 제작법이나 Malware 개발과 같은 질문에 대해서는 거부하는 경향이 있지만 프롬프트 엔지니어링 기법을 사용하여 원하는 답변을 얻거나 해킹에 도움이 되는 코드를 생성하려는 해커들의 시도가 빈번하게 발생하고 있다.

4. 결 론

인공지능(AI)을 적용한 지방자치단체 물리적 보안 개선 방안을 살펴 본 결과, 잠재적인 위험 예측 및 사전에 범죄 예방, 상황에 맞는 보안조치 추천, 보안 인력의 업무 효율성을 향상시키는 등 인공지능(AI)은 청사의 물리적 보안을 개선하는 데 효과적인 기술로 나타나는 것을 알 수 있다. 다만, 인공지능(AI)을 적용 하는데 기술적인 한계와 보안 취약 문제 등을 보완해 나간다면 지방자치단체 청사의 물리적 보안을 보다 효과적으로 개선될 뿐만 아니라, 나아가서 청사를 이용하는 일반 시민과 일선 공무원들을 악성 민원인과 범죄로부터 사전에 차단하고 보호 받을 수 있을 것으로 기대한다.

참고문헌

데이터헌트, 보안 AI 인공지능, 활용 사례와 적용 기술, https://www.thedatahunt.com/trend-insight/ai-in-security, 2023년 10월 16일

“지자체 도입으로 살펴본 선별과제의 오늘과 내일”, 보안뉴스, 2019년 3월 5일