AI 디지털 교과서의 보안 취약성과 국가 교육 시스템의 운영에 미치는 영향 분석

김민주, 김아영, 송종근*
동서대학교, *동서대학교
20230744@office.dongseo.ac.kr, 20230755@office.dongseo.ac.kr, *ssongig@dongseo.ac.kr

An Analysis of Security Vulnerabilities in AI Digital Textbook and Their impact on the Operation of the National Education System

Kim Min Ju, Kim A Yeong, Song Jong Gun*
Dongseo Univ., *Dongseo Univ.

요 약

본 논문은 인공지능(AI) 디지털 교과서(AIDT)의 본격적인 도입을 앞두고, 클라우드 기반 중앙 집중형 플랫폼이 내포하는 보안 취약점과 이에 따른 국가 교육 시스템 운영의 리스크를 심층적으로 분석하였다. AIDT는 학생 맞춤형 학습을 위해 성취 수준, 학습 경로, 오류 패턴 등 민감하고 방대한 학습 데이터를 수집하며, 이 데이터는 국가 주도의 '학습데이터 허브'로 통합 관리되는 중앙 집중형 구조를 갖는다. 이러한 구조는 해킹 발생 시 전국적인 교육 시스템 마비 또는 대규모 학생 정보 유출로 인한 공교육 신뢰도 붕괴 위험을 내포한다. 분석 결과, AIDT 해킹은 단순히 데이터 유출을 넘어 AI 알고리즘 변조 및 데이터 오염을 통해 맞춤형 학습 기능 자체를 근본적으로 훼손할 수 있음이 확인되었다. 따라서 본 논문은 이러한 위협을 이 어떠한 경로로 발생할 수 있고, 어떠한 결과를 불러일으킬 수 있을지 분석하였다.

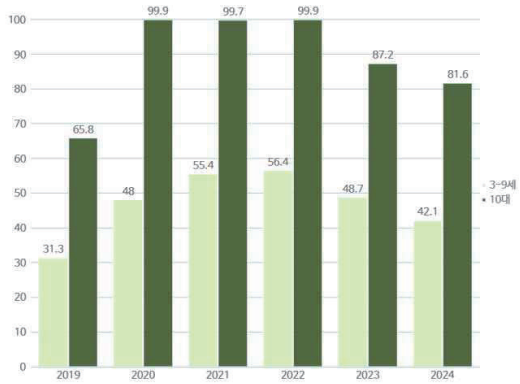
Ⅰ. 서론

AI 디지털 교과서(AIDT)란 학생 개인의 능력과 수준에 맞는 다양한 맞춤형 학습 기회를 지원하고자 인공지능을 포함한 지능정보기술을 활용하여 다양한 학습자료 및 학습 지원 기능 등을 탑재한 소프트웨어로 AI에 의한 학습 진단과 분석(Learning Analytics), 개인별 학습 수준과 속도를 반영한 맞춤형 학습(Adaptive Learning), 학생의 관점에서 설계된 학습 코스웨어(Human-Centered Design) 기능이 존재한다.

AIDT 도입의 기대 효과는 학생들의 사회·문화·경제적 배경과 관계없이 신기술에 접근성을 보장하고 개별 맞춤 교육 기회를 갖도록 설계하여 교육 기회의 균등화를 이룬다. 이러한 시스템은 개별 맞춤형 학습 지원과 AI 보조교사 기능 제공으로 학습 효율성을 극대화할 것으로 전망된다.

이러한 공교육 환경에서의 디지털 교육으로 전환은 COVID-19 사태를 기점으로 급격히 가속화되었다고 볼 수 있다.

이와 관련하여, 아래 그래프는 COVID-19 이후 연도별 3~9세 및 10대 연령층의 온라인 교육 이용 추이를 정리한 것이다.



출처 : NIA, 인터넷이용실태조사 참조해 필자 작성

위 그래프에서 알 수 있듯이 인터넷 교육 사용량이 과거에 비해 현저히 증가하였고, 현재 AIDT의 본격적인 도입을 앞두고 있다.

본 논문은 이러한 AIDT 시스템의 본격 도입에 앞서, 제도적 불안정성과 기술적 보안 리스크라는 두 가지 핵심 구조적 취약점을 분석하고 사고 예방 방안을 모색하는 것을 목적으로 한다.

Ⅱ. 본론

AIDT 시스템은 교육과정에 따른 유연한 운용과 확장성을 위해 클라우드 기반의 SaaS(Software as a Service) 모델로 구현된다. 기술적 구조의 핵심은 학생들의 모든 활동 데이터를 통합 저장하는 학습 데이터 허브(Learning Data Hub)이다.

[AI 디지털교과서 서비스 구성도]
출처 : AI·디지털 교육자료 통합지원센터

이 허브는 교육과정 표준체계를 통해 국가 교육과정을 성취 기준 및 평가 루브릭과 같은 정량적 데이터로 표준화하고, 이를 민간 개발사가 제공

하는 AI 진단평가, AI 튜터 등 맞춤형 서비스와 연동한다. 궁극적으로 이 아키텍처는 중앙 집중화된 데이터를 기반으로 학생 개개인에게 맞춤형 학습을 동적으로 제공하는 기술적 인프라를 구축한다.

AIDT는 개인별·과목별 고유식별값(UUID) 체계를 갖추고 국가정보원 보안점검 및 클라우드 보안인증(CSAP)을 획득하는 등 기본적인 보안 조치를 구비하고 있다. 그러나 개인정보보호 위원회의 2025년 사전 실태 점검 결과, 개인정보 안전성 확보를 위한 검정 심사 기준과 개발 가이드라인이 클라우드 보안 측면에 치우쳐 있어 보호법상의 안전조치에 대한 고려가 미흡한 것으로 확인되었다. 특히 우려되는 점은 참여자 간 시스템 연동(API 연계 등) 과정에서 보안 취약성과 공급망 공격을 통한 시스템 침투이다. 학습 데이터 허브를 중심으로 80여 개의 출판사와 다수의 에듀테크 기업들이 연계되는 복잡한 생태계 구조는, 각 연결 지점마다 잠재적 공격 표면을 형성한다.

*API 보안 취약점

AIDT 통합 포털과 각 개발사 웹사이트 간의 API 연동 구조는 필수적이지만, API 인증 정보의 노출이나 권한 제어의 부재는 무단 접근의 주요 경로가 된다. 인터페이스나 API는 기능 명세 이외에 기능이나 보안 위협들을 식별하기 어렵기 때문에 이러한 연동 구조의 보안 취약성을 인지하고, 소프트웨어 개발 시에 시큐어 코딩 적용 및 WAAP솔루션을 적용해야 한다.

*공급망 공격(Supply Chain Attack)을 통한 시스템 침투

클라우드 저장소 데이터 유출은 보안 아키텍처를 대상으로 하는 '공급망 공격(Supply Chain Attack))'에 의해서 발생한다. 단일 개발사 또는 에듀테크 기업의 시스템 침해는 연쇄적인 보안 사고로 확대될 위험이 존재한다. 공격자가 하나의 개발사 계정을 탈취하면, API 연동을 통해 중앙 학습 데이터 허브로의 접근 권한을 획득할 수 있으며, 이는 전국 규모의 학생 데이터 유출로 이어질 수 있다.

AIDT의 가장 본질적인 보안 위험은 학습 데이터 허브라는 중앙 집중형 구조 자체에 있다. 이 구조는 대규모 개인정보 유출의 위험 · 공교육 시스템의 마비와 신뢰도 붕괴 등 연쇄적 위험을 내포하고 있다.

Ⅲ. 결론

본 논문에서는 AI 디지털 교과서(AIDT)의 중앙 집중형 클라우드 아키텍처가 내포하는 보안 취약점을 다각도로 분석하였다.

분석 결과, AIDT는 교육과정 표준체계와 학습 데이터 허브(Learning Data Hub)를 중심으로 설계된 혁신적인 아키텍처를 기반으로 맞춤형 학습을 실현할 잠재력을 충분히 갖추고 있다. 이 시스템은 인공지능 기반의 진단 및 분석을 통해 학생 개개인의 성취도와 학습 속도를 반영하여 교육 형평성을 제고하고 학습 효율성을 극대화하는 새로운 교육 패러다임을 제시한다.

그러나 현재의 보안 체계는 클라우드 인프라 보안에 과도하게 집중되어 있으며, API 연동 구조와 데이터 처리 과정에서의 보안 조치는 상대적으로 미흡하다. API로 연동되는 복잡한 생태계는 공급망 공격에 취약하며 단일 지점의 침해가 연쇄적 보안 사고로 전국적 규모의 교육 마비로 확산될 위험이 있다.

또한, 학생들의 민감한 학습 이력 및 진단 정보를 중앙 집중식으로 관리하는 학습 데이터 허브는 해킹 시나리오 분석 결과, 개인정보의 기밀성과 학습 데이터의 무결성에 대한 중대한 위협을 내포한다. 특히 민간 개발사 인프라를 통한 공급망 공격 가능성과 공공 포털의 인증 우회 취약점은, 학생들의 개인정보 자기결정권을 침해하고 학습 데이터를 변조하여 공교육의 신뢰를 붕괴시킬 수 있는 리스크를 증폭시킨다.

따라서 이러한 문제를 방지하기 위해서는 제로 트러스트(Zero Trust) 보안 모델의 도입, API 보안 강화, 분산형 데이터 관리 체계 구축 등 근본적인 보안 아키텍처 재설계가 시급하다.

결론적으로, AIDT가 당초 목표했던 미래 교육 혁신을 달성하기 위해서는 정책 추진의 '속도' 경쟁을 중단하고 '신뢰'와 '안정성' 확보로 정책의 방향을 근본적으로 전환해야 한다.

본 연구는 AIDT의 기술적 구조와 보안 취약점을 이론적으로 분석한 것으로, 향후 실제 시스템에 대한 침투 테스트와 취약점 점검을 통한 실증적 연구가 후속되어야 할 것이다. 또한 교육 데이터의 특수성을 고려한 프라이버시 보호 기술(Privacy-Preserving Technology)의 적용 방안에 대한 심층 연구가 필요하다.

ACKNOWLEDGMENT

이 논문은 2025년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임 (P0024163, 2025년 지역혁신클러스터 육성)

참 고 문 헌

[1] AI · 디지털 교육자료 통합지원센터, "AI 디지털 교과서 개발 가이드라인" (https://aidt.keris.or.kr/aidt/main.page)

[2] 황현주. (2024). 데이터로 살펴본 디지털 교육혁신 현황 - AI 디지털 교과서를 중심으로. 한국지능정보사회진흥원.

[3] NIA, 2024_인터넷이용실태조사

[4] 조용기, "인공지능 디지털교과서(AIDT) 도입의 문제점 및 개선 방안," 종교교육학연구, 80, 91-108, 2025, 10.58601/kjre.2025.03.30.06.

[5] 이글루코퍼레이션. (2023.5.17). 클라우드 환경의 보안사고 사례분석을 통한 대응방안. (https://www.igloo.co.kr/security-information)

[6] 디지털투데이. (2025.5.15). AI 디지털교과서 개인정보보호 실태 조사 결과 발표. (http://digitaltoday.co.kr/news/articleView.html?idxno=566312)