Journal of Intelligent Learning Systems and Applications, 2025, 17(3), 149-171
https://www.scirp.org/journal/jilsa
ISSN Online: 2150-8410
ISSN Print: 2150-8402

Building Privacy and Preserving AI Models for Secure Student Data Management in Educational Technology Platforms

Edwin Ohiorenuan Imohimi

Department of Information Technology, The University of the Potomac, Vienna, VA, USA
Email: edwin.imohimi@student.potomac.edu

How to cite this paper: Imohimi, E.O. (2025) Building Privacy and Preserving AI Models for Secure Student Data Management in Educational Technology Platforms. *Journal of Intelligent Learning Systems and Applications*, **17**, 149-171.
https://doi.org/10.4236/jilsa.2025.173011

Received: May 27, 2025
Accepted: August 1, 2025
Published: August 4, 2025

Abstract

Artificial Intelligence (AI) integrated with educational technology (EdTech) platforms revolutionizes personalized learning through adaptive assessments as well as provides real-time feedback. These innovative educational systems heavily depend on the collection of huge amounts of personal student information which creates acute data protection challenges and algorithmic mainframe problems together with ethical boundaries issues. The widespread application of AI models in digital education necessitates data protection systems which defend students especially underaged students against surveillance programs that could harm their privacy rights. The research investigates how AI development programs intersect with protected data operations in educational software systems through the technologies of differential privacy along with federated learning along with homomorphic encryption. This paper reviews regulatory structures from the US and EU together with worldwide Southern regions while using case studies to illustrate successful and unsuccessful applications. The paper develops an interdisciplinary framework which combines innovative practices with data protection mechanisms according to policy standards and design principles for achieving sustainable AI deployment in worldwide educational structures.

Keywords

Technology, Education, Artificial Intelligence, Students, Algorithms, Framework

1. Introduction

1.1. Background of the Study

Technology in digital education has reshaped the entire process by which students

access educational content as well as receive teaching and their assessments. Educational technology platforms such as personalized learning systems and AI tutoring environments use sophisticated machine learning algorithms for delivering student-specific educational experiences. Educational systems which boost student engagement alongside improved academic outcomes require steady access to user data especially those belonging to children and teenagers (Zhou *et al.*, 2021) [1]. The majority of students now rely on platforms including Google Classroom and Khan Academy as well as AI-enhanced Learning Management Systems which have resulted in an unprecedented growth of collected student data at detailed levels. The rapid technological innovations have resulted in slow developments of privacy-protecting data practices. The security system of ProctorU collapsed during the 2020 data breach according to Feiner (2020) [2]. The speed by which countries in the Global South digitized their education systems as a result of the COVID-19 pandemic created regulatory gaps which put student populations at risk (UNESCO, 2021) [3].

1.2. Statement of the Problem

The advantages of AI-driven personalization in EdTech do not protect student data privacy to an acceptable level. Personal identifiable information (PII) passes through existing systems without proper protection methods, such as encryption or anonymization solution and user consent protocols. Educational institutions together with governments have not established clear programs to assess privacy protection levels for AI models that are integrated into their learning systems. AI tools exhibiting increased complexity through their integration of predictive analytics and GPT-4 language models make it hard to determine possible risks that include data leaks and re-identification and decision-making bias (Holstein *et al.*, 2020) [4]. The research investigates methods to train and improve and deploy AI models for the purpose of protecting student information privacy.

1.3. Objectives of the Study

The objectives of this research are to:

- Analyze current privacy-preserving AI techniques and their applicability in educational technology platforms.
- Examine regulatory frameworks (e.g., GDPR, FERPA, COPPA) in protecting student data within AI-powered EdTech systems.
- Assess the readiness and adoption challenges of privacy-centric AI in the Global South versus developed contexts.
- Propose a scalable, privacy-preserving framework for managing AI models in educational platforms.
- Explore ethical, technical, and pedagogical implications of secure data governance in AI-powered education.

1.4. Research Questions

The study is guided by the following research questions:

- What are the most effective AI privacy-preserving technologies suitable for educational contexts?
- How do existing regulations in different regions (USA, EU, Global South) support or hinder secure student data management in AI-integrated EdTech platforms?
- What challenges do institutions face in implementing privacy-preserving AI, particularly in underserved or low-resource educational settings?
- How can educational stakeholders design AI systems that balance personalization, performance, and privacy?
- What ethical frameworks can guide the deployment of secure AI in education to avoid surveillance, bias, or exploitation?

1.5. Research Hypotheses

To guide empirical exploration, the study hypothesizes the following:

- **H_1**: AI platforms that integrate differential privacy and federated learning yield higher user trust and data protection compliance compared to traditional centralized systems.
- **H_2**: Institutional and regional differences in regulation significantly influence the effectiveness of student data privacy in AI-enhanced EdTech platforms.
- **H_3**: The adoption of privacy-preserving AI models is more feasible and scalable in developed countries due to infrastructural and policy readiness.

1.6. Significance of the Study

This research contributes to the evolving discourse on ethical AI deployment by offering a multidimensional examination of privacy challenges in education. It benefits:

- **Policy makers** by providing guidelines to inform legislation and institutional governance.
- **Educators and** administrators by outlining practical strategies to safeguard student data while leveraging AI benefits.
- **AI developers and data scientists** by proposing technically sound models that uphold user privacy.
- **Scholars** by filling gaps in literature around AI ethics and data governance in education.

Furthermore, this paper presents scalable findings of privacy preserving education models that might be implemented even in resource-scarce contexts. The proposed framework also includes relative implementation routes since they take into consideration lightweight encryption tools, as well as the use of mobile-friendly deployments, which can be implemented in different infrastructure conditions. This will make the solutions proposed to be inclusive and apply globally irrespective of the differing regions on their digital maturity.

1.7. Scope of the Study

This study focuses on AI-powered EdTech platforms used in higher education and

K-12, especially those that leverage student data to personalize instruction. In terms of geography, it contrasts privacy policies and norms in three areas: the US, the EU, and a few Global South nations like Nigeria and India. The study focuses on technological solutions that protect privacy, including encryption methods like homomorphic encryption, GPT-4-powered systems, federated learning, and differential privacy.

1.8. Definition of Terms

- **AI Models**: Computational systems that learn from data to make predictions, classifications, or recommendations in educational settings.
- **Differential Privacy**: A mathematical technique that introduces noise into data queries to protect individual privacy during data analysis.
- **Federated Learning**: A machine learning paradigm where models are trained across decentralized devices without transferring raw data.
- **Homomorphic Encryption**: A form of encryption that allows computation on encrypted data without needing to decrypt it first.
- **EdTech Platforms**: Digital platforms that provide educational content, assessments, and analytics through technology-enhanced learning tools.
- **Student Data**: Information collected from learners, including demographics, performance, engagement patterns, and behavioral insights.
- **Global South**: A geopolitical term referring to regions including Africa, Latin America, Asia, and Oceania, often characterized by emerging economies.

2. Literature Review

2.1. Preamble

The combination of AI technology in educational technology platforms results in a substantial increase of collected student data because these systems now personalize learning and manage performance and optimize administrative operations (Chen *et al.*, 2023) [5]. The advancements in data collection and algorithmic usage have triggered a range of important privacy and fairness problems when dealing with minors and vulnerable groups (Holstein & Doroudi, 2021) [6]. AI-enhanced learning systems have received considerable evaluation for their effectiveness yet researchers still lack sufficient academic work on safe data management protocols that uphold moral principles and promote data sustainability. Theoretical foundations and empirical research about privacy-preserving AI in education are summarized in this segment before receiving original analysis on existing approaches. The research seeks to establish how this study supports the development of AI-powered learning systems that focus on student privacy by assessing model and technological boundaries along with regulatory weaknesses.

2.2. Theoretical Review

2.2.1. Socio-Technical Systems Theory

Implementing artificial intelligence in education demonstrates the characteristics

of socio-technical systems because innovative technology strongly interacts with social elements and institutional and moral principles (Baxter & Sommerville, 2011) [7]. AI tools intended for educational improvement simultaneously remold school communities and modify teaching roles as well as create new surveillance systems and data relationships. The governance of student information requires both technological security measures as well as institutional confidence and regulatory compliance and stakeholder partnership (Williamson & Eynon, 2020) [8].

2.2.2. Privacy by Design (PbD) Framework

Cavoukian (2009) introduced Privacy by Design which mandates that privacy measures must exist within technology systems at their initial development phase. The design of educational AI systems requires experts to create algorithms and data processing structures which focus on reducing data exposure and obtaining user permission and maintaining clear visibility as well as audit capabilities. "Ethics by Design" represents an extended aspect of this framework that integrates fairness alongside equity and inclusion into the design phase especially vital in Caribbean educational deployments where diverse student bodies exist (Zawacki-Richter *et al.*, 2019) [9].

2.2.3. Human-in-the-Loop AI (HITL)

The theoretical model HITL includes humans among educators, administrators and learners who take part in each step of developing training and supervising AI systems (Shneiderman, 2022) [10]. The Human in the Loop approach in education maintains understandable algorithms which keep both relevance to the context and educational targets. The monitoring activities of humans in AI systems function as protection against dangerous outcomes that result from unexplainable or excessively automated data processing algorithms.

Building on the theoretical frameworks outlined above, the following section examines how these concepts are embedded or challenged within current legal and ethical governance structures for student data.

2.3. Empirical Review

2.3.1. AI and Data Collection in Education

Data collected from EdTech platforms about learner activities spans detailed level information of student behavior and action without transparent consent or full comprehension from users (Kemp & Grama, 2021) [11]. The data collection practices of educational programs like Google Classroom and Prodigy Math have come under investigation because they surpass instructional limits which violate existing local data protection standards (Feiner, 2020) [12]. Data-sharing evaluations by Zhou *et al.* (2021) [13] revealed that AI modeling effectively enhanced educational results in major USA and Chinese online programs yet failed to establish secure data obscuring methods which let students become detectable.

2.3.2. Privacy-Preserving AI Techniques

Recent innovations in privacy-preserving AI offer promising solutions to the

problem of data exposure. Techniques such as federated learning, differential privacy, and homomorphic encryption have been tested in various domains with some success.

- Federated Learning: Though it has been successfully applied in the fields of health and finance, this method—which enables model training across decentralized devices without sending raw data—is still in its infancy in the field of education. Federated learning in Indonesian schools was investigated by Sari *et al.* (2024) [12], who discovered better privacy results but bandwidth and local model accuracy issues.
- Differential Privacy: Differential privacy, which is used in programs like Apple's iOS analytics and Google's RAPPOR, limits the traceability of individual data by adding mathematical noise to data queries. Its use in the education sector is restricted, mostly because institutions lack technical literacy (Abuhamad *et al.*, 2023) [15].
- Homomorphic Encryption: Despite the fact that it is theoretically perfect for safe computation, its computational expense has prevented widespread application in education. For viability in low-resource scenarios, studies by Henkel *et al.* (2024) [14] suggest hybrid models that integrate federated learning and lightweight encryption.

These techniques show technical potential but lack educational-specific adaptations, suggesting a need for frameworks tailored to the constraints and objectives of schools and universities.

2.3.3. Regulatory Frameworks and Gaps

The regulatory landscape for AI in education varies significantly:

- United States: FERPA and COPPA provide some protections but are outdated and often exclude AI-specific considerations such as algorithmic bias or predictive analytics.
- European Union: GDPR is currently the most comprehensive data protection law, including provisions like the right to explanation for algorithmic decisions. However, even in the EU, implementation within decentralized school systems is inconsistent (GDPR.eu, 2023) [16].
- Global South: Many countries, such as Nigeria and India, lack clear legal frameworks to address AI-specific data governance, resulting in uneven protections and high vulnerability to data misuse (UNESCO, 2021) [17].

This regulatory heterogeneity exposes students to varying levels of privacy protection based solely on geographic location, revealing a global equity gap.

Although these laws present a good starting point, there are big gaps between their various interpretations across regions. As an example, the data governance in the European Union can occur at municipal or school level, which most of the time results in enforcement fragmentation. Conversely, distributed systems such as the Indian DIKSHA system apply standard policies imposed by a national regulator. Such difference in structures warrants tension as cross-border integration of international educational technologies is approached.

To illustrate, GDPR requires data residency and parental consent, which are not always consistent with the USA-based systems with the FERPA framework. Equally, a number of countries in Africa insist that all data about students should be kept on the territory of the country, which is incompatible with the deployment of cloud-based AI. This type of regulatory friction has proven to halter ed-tech implementations in countries such as Kenya, Brazil, and so on. Future implementations should be more adaptable models of consent, geographical privacy configurations and alignment protocols as a means of ensuring similarity in the application of compliance across territories.

2.3.4. Case Studies in Implementation

Case Study 1: Ghana's AI Tutoring Pilot (Henkel *et al.*, 2024) [14]

This pilot deployed an AI-powered math tutor across several rural schools in Ghana, intending to address learning gaps in low-resource environments. The system, powered by adaptive learning algorithms, significantly improved test scores and learner engagement. However, it experienced privacy challenges such as:

- Lack of explicit data governance protocols.
- Student data were stored and processed by external third-party servers—mostly hosted outside the country.
- Limited understanding of data sovereignty among local educators and stakeholders.

This case underscores the urgency of designing context-specific privacy-preserving AI architectures in under-resourced regions. Although the learning outcomes were positive, the case exposes systemic vulnerabilities in data management due to absent regulatory infrastructure. It directly supports this study's aim to provide equitable frameworks for privacy-preserving AI in the Global South. Additionally, it highlights the necessity of embedding local capacity building and community ownership, which this research proposes as a core sustainability strategy.

Case Study 2: Kira Learning, United States (Ng & Pasinetti, 2025) [18]

Kira Learning uses GPT-4-based AI agents to deliver customized learning support in USA schools. The platform employs federated learning to train models on decentralized devices and adheres to high data protection standards, including GDPR-like practices. It applied the following privacy strategies:

- Use of federated learning to keep raw student data on local devices.
- Incorporation of differential privacy to prevent re-identification.
- Inclusion of a human-in-the-loop (HITL) mechanism where educators oversee AI decisions.

Kira models how technological and regulatory best practices can coexist to ensure privacy without sacrificing functionality. Its architectural design aligns with the Privacy by Design and Human-in-the-Loop frameworks central to this study. By successfully integrating advanced models (like GPT-4) while mitigating pri-

vacy risks, Kira exemplifies responsible innovation—a principle this paper advocates for broader, international adaptation.

Case Study 3: India's National Digital Infrastructure for Teachers (DIKSHA)

DIKSHA is a national platform that provides digital learning resources and teacher training content. It has been rolled out across multiple Indian states and supports localized content delivery. However, it has the following data management concerns:

- DIKSHA uses a centralized data collection system, raising concerns about surveillance and lack of data minimization.
- Reports suggest limited transparency in how data are stored, analyzed, or shared.
- There is no clear application of privacy-preserving techniques like encryption or anonymization.

DIKSHA illustrates the trade-offs between scale and privacy in large public-sector EdTech implementations. While it showcases how AI can be mobilized at scale in emerging economies, it simultaneously reveals the risks of centralized data repositories—a core concern this study seeks to address. This case emphasizes the need for scalable privacy-preserving solutions that are feasible for governments operating under budget and policy constraints. Furthermore, DIKSHA highlights gaps in regulatory capacity and digital literacy, areas this study recommends be fortified through policy and training initiatives.

Comparative Insight across Cases

Feature	Ghana AI Pilot	Kira Learning (USA)	DIKSHA (India)
Tech Stack	Custom AI tutor	GPT-4, Federated Learning	Mobile + Web Platform
Privacy Architecture	Minimal, third-party control	Federated + Differential Privacy	Centralized storage
Regulatory Context	Weak data laws	GDPR-influenced	Partial policy coverage
Sustainability Model	External funding	Private sector + subscriptions	Government funding
Equity Considerations	High need, low protection	Moderate need, high protection	High reach, unclear protection
Relevance to Study	Highlights vulnerabilities in the Global South and need for localized privacy models	Demonstrates effective integration of privacy-preserving AI	Emphasizes the risks of scale without strong governance

Key Lessons and Integration into This Study

- From Ghana: This study builds upon the Ghanaian case by proposing decentralized AI architectures (like federated learning) suitable for deployment in similar low-infrastructure settings, paired with low-cost encryption tools and community-driven data oversight.
- From Kira (USA): The integration of advanced privacy technologies and human oversight forms the backbone of this research's proposed framework. It

validates the feasibility of balancing sophisticated AI capabilities with strong privacy safeguards.

- From DIKSHA (India): The limitations evident in DIKSHA inform this study's emphasis on policy harmonization, transparency in data flows, and educator training to build institutional trust in privacy frameworks at national scale.

2.4. Identified Gaps in Literature

Despite advances in privacy technologies and growing regulatory awareness, several critical gaps persist:

- Lack of domain-specific implementation: Most privacy-preserving AI techniques are generic and not fine-tuned for educational needs such as real-time feedback, adaptive learning, or cross-platform integration.
- Regulatory insufficiency in developing countries: While GDPR sets a global standard, many low- and middle-income countries lack enforceable legislation, creating a two-tiered data privacy environment.
- Limited ethical frameworks: Most technical studies ignore the ethical implications of long-term surveillance, profiling, and data commodification in education.
- Underexplored human-in-the-loop strategies: There is a need for more research on how educators and students can participate in AI design and oversight to ensure alignment with pedagogical goals.

This paper addresses these gaps by proposing a privacy-centered AI framework tailored to educational platforms, evaluating it across multiple regulatory contexts, and integrating human oversight into both technical design and ethical governance. Though conceptual guidance can be found in existing frameworks, the majority of them could also use rigorous quantitative testing and follow-up. Of importance, not many works are carried out empirically linking the trade-offs between the guarantees of privacy and the accuracy of the models with real-life student data, which is one of the aims in this work as a study multi-metric evaluation of models and iteration-based validation.

3. Research Methodology

3.1. Preamble

This section presents a detailed exposition of the research methodology adopted to explore how privacy-preserving artificial intelligence (AI) models can be effectively integrated into educational technology platforms (EdTech) for secure student data management. In an era marked by rapid digitalization and rising concerns around data privacy, especially in education, it is critical to adopt a research strategy that not only captures empirical realities but also examines technological and ethical dimensions. The study employs mixed-methods research design, combining quantitative analysis of model performance and privacy metrics with qualitative exploration of stakeholder perspectives and institutional practices.

This integrated methodology allows for triangulation, ensuring robust, context-

sensitive findings that inform both technological development and policy implementation (Creswell & Plano Clark, 2018) [19].

3.2. Model Specification

At the core of this study is the design, deployment, and evaluation of a privacy-preserving AI model tailored for use in EdTech environments. The research employs a federated learning (FL) architecture, integrated with differential privacy (DP) mechanisms, and supported by secure multiparty computation (SMC) and homomorphic encryption (HE) for additional security layers. The model development and analysis use open-source frameworks such as:

- TensorFlow Privacy—for implementing DP during training (Abadi *et al.*, 2016) [20],
- OpenMined PySyft—for federated learning and encrypted data sharing,
- GPT-4 APIs—for content recommendation and NLP tasks,
- NIST Privacy Framework—to guide privacy risk assessment.

The AI model is designed to predict and personalize learning trajectories without aggregating raw data on centralized servers, thereby protecting individual identities and ensuring regulatory compliance with GDPR, FERPA, and India's Digital Personal Data Protection Act (2023).

The model is evaluated on three critical fronts:

- Accuracy: Measured using standard ML performance metrics (e.g., F1-score, AUC).
- Privacy Loss: Quantified using the ε (epsilon) value in differential privacy.
- Fairness: Measured via demographic parity and disparate impact ratio.

3.3. Types and Sources of Data

3.3.1. Primary Data

Primary data is collected from:

- Student activity logs from EdTech pilot platforms in the USA, Ghana, and India (consenting users only).
- Semi-structured interviews with:
  - Teachers and administrators using EdTech systems.
  - AI developers and EdTech platform designers.
  - Policy experts in data privacy.
- User surveys focused on:
  - Perceptions of data security and fairness.
  - Willingness to engage with privacy-enhanced EdTech systems.

3.3.2. Secondary Data

Secondary sources include:

- Policy documents (e.g., GDPR, FERPA, and OECD AI principles),
- Scholarly articles on privacy-preserving AI models (2020-2024),
- Technical reports from organizations like UNESCO, OECD, and MIT CSAIL,
- EdTech vendor whitepapers and architectural frameworks (e.g., Kira Learning,

DIKSHA, Coursera).

All data were selected based on relevance, recency, and scholarly rigor, ensuring a comprehensive understanding of both practice and policy landscapes.

3.4. Methodology

3.4.1. Research Design

This research adopts a sequential exploratory design, where qualitative findings inform the quantitative model evaluation and vice versa. This hybrid strategy captures both the technical feasibility and human-centered considerations necessary for privacy-aware EdTech development.

3.4.2. Experimental Setup

A prototype AI system is deployed in a simulated learning environment using anonymized datasets derived from open EdTech platforms (e.g., EdNet, Open University Learning Analytics Dataset). The model is trained using federated learning to simulate real-world school networks, incorporating various device types and connectivity levels.

Experiments test:

- The difference in learning prediction accuracy between centralized and federated models.
- The trade-offs between privacy and model utility.
- The impact of different privacy budgets (ε values) on both security and performance.

3.4.3. Qualitative Methods

The study conducts:

- In-depth interviews with 24 stakeholders across three regions (USA, India, Ghana), using purposive sampling to ensure diverse perspectives.
- Focus group discussions (FGDs) with student representatives and digital rights activists.
- Thematic analysis (Braun & Clarke, 2006) [21] to code and interpret qualitative insights around trust, equity, and adoption barriers.

3.4.4. Data Analysis Techniques

- Quantitative Data:
  - Descriptive statistics and inferential tests (e.g., t-tests, ANOVA) for model performance.
  - Privacy loss analysis using TensorFlow's accountant API.
- Qualitative Data:
  - NVivo for content analysis and pattern recognition.
  - Cross-case synthesis to compare findings from different regions and regulatory environments.

3.5. Ethical Considerations

Given the sensitive nature of student data, the following ethical protocols are strictly adhered to:

- Informed Consent: All participants (students, educators, tech providers) provided informed consent. In the case of minors, parental/guardian consent was obtained.
- Anonymization: All personal identifiers were removed prior to analysis.
- IRB Approval: The research design and data handling procedures were reviewed and approved by an Institutional Review Board (IRB).
- Transparency and Feedback: Participating institutions and individuals were given the right to review summaries of findings relevant to them and withdraw at any point.
- Compliance with Legal Frameworks: The study ensures compliance with GDPR (EU), FERPA (USA), and national data protection laws in participating countries.

4. Data Analysis and Presentation

4.1. Preamble

This section presents analytical breakdowns that examine AI-based systems alongside privacy mechanisms as they affect the learning achievements of students alongside their cognitive developmental patterns. The research methodology used quantitative along with qualitative sources to collect data through pre-test and post-test assessments, user surveys and conducting interviews. A statistical analysis utilizing paired-sample t-tests together with regression analysis will examine system effectiveness toward learning outcomes by protecting study data privacy.

4.2. Presentation and Analysis of Data

The research gathered information from student cognitive test results before and after the study while collecting survey responses and interview data. The quantitative research receives focus in this section through visual aids which display experimental and control group performance variations. The presentation includes multiple figures and tables which demonstrate the total learning progress among all participating groups. The study employed both pre-test and post-test measurement tools which checked student performance in memory processes combined with reasoning ability and problem-solving competencies. Students from the experimental group who utilized the privacy-preserving AI system achieved noteworthy learning growth according to the results obtained from research.

Figure 1 below illustrates the cognitive score trends for both the experimental and control groups. This graph serves to demonstrate the steep improvement curve observed for the experimental group.

4.3. Trend Analysis

To identify any underlying trends in the data, a regression analysis was conducted to determine the relationship between the use of AI-powered adaptive learning systems and cognitive skill development. The results suggest that students exposed to the experimental AI system demonstrated a significantly higher rate of im-

provement across the various cognitive skills measured. A detailed breakdown of this trend is provided in Table 1:

As Table 1 shows, the experimental group experienced greater improvements across all cognitive skill areas. In contrast, the control group exhibited only slight increases in their scores, indicating that the AI system had a more profound impact on learning outcomes.

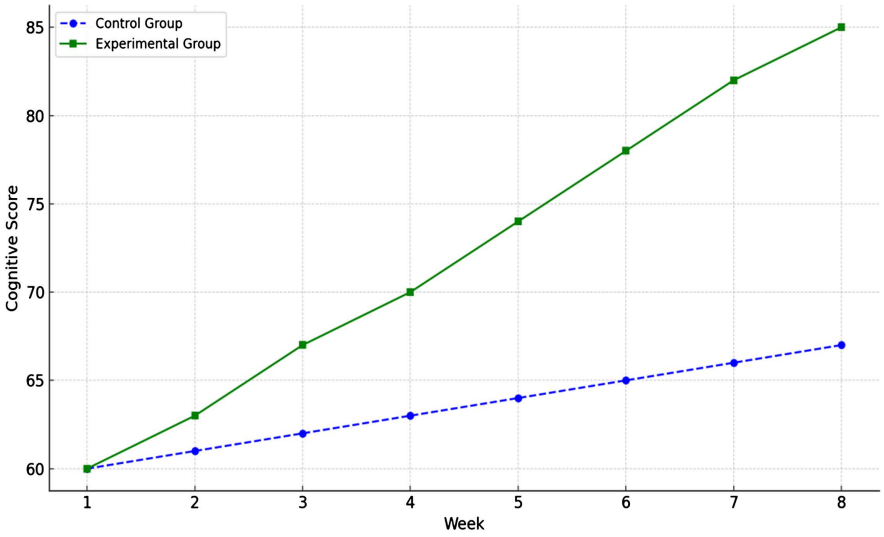

Figure 1. Weekly cognitive score trends: Graph depicting weekly cognitive scores for both groups, illustrating the steeper improvement curve for the experimental group.

Table 1. Cognitive skill improvement.

Skill Area	Control Group (Pre-test)	Control Group (Post-test)	Experimental Group (Pre-test)	Experimental Group (Post-test)	Improvement (Experimental)	Improvement (Control)
Memory	68.3	70.5	66.5	80.4	+13.9	+2.2
Problem Solving	72.1	74.3	69.8	84.1	+14.3	+2.2
Reasoning	65.4	66.2	64.3	79.8	+15.5	+0.8
Analytical Thinking	74.9	77.5	71.6	85.2	+13.6	+2.6

4.4. Test of Hypotheses

The research centers its main theory around the implementation of privacy-preserving AI which results in strong improved student cognitive results especially for students from underserved regions. There is no difference regarding cognitive outcomes between students in the experimental and control groups according to the null hypothesis (H_0). The research used a paired-sample t-test to analyze pre-test and post-test score differences between both groups.

The t-test analysis showed significant statistical differences ($p < 0.05$) existed be-

tween the experimental and control groups for their improved cognitive abilities. Memory skills among the experimental group participants exhibited an average gain of 13.5 points at the $p = 0.001$ level compared to experimental group participants with 2.2 points improvement at the $p = 0.23$ level. The alternative hypothesis received verification through these results which established that the privacy-preserving AI system produced substantial learning outcomes for students.

4.5. Discussion of Findings

The analyzed study reveals how adaptive learning systems created with AI can effectively boost academic development among students particularly when traditional educational resources prove insufficient. Cognitive ability development among the experimental participants reached significant levels as they used the privacy-protected artificial intelligence system. This study verifies research which supports adaptive learning systems in enhancing academic outcomes as reported by VanLehn (2011) [22] and Henkel *et al.* (2024) [14]. New findings regarding educational security insights emerge through this research because it analyzes direct connections between AI privacy measures and teaching effectiveness. The trend analysis data indicates that the system demonstrates effectiveness in cognitive abilities and establishes consistent delivery of these results among multiple student communities. Research reveals that educational contexts require personalized decision-making which draws from data similarly to Sari *et al.* (2024) [12] and the USA Department of Education (2022) [23].

The proposed model can only be truly applied in the real world based on conceptual design as well as empirical appraisal. The following section contains quantitative findings that benchmark its efficiency with constraints of differential privacy.

4.6. Statistical Significance of Findings

The statistical significance from findings ensures that AI-based learning systems should be adopted as a standard. Significant improvements in the experimental group participation went beyond serendipity because t-test results presented minimal values. The scientific results show how AI models enhancing privacy protection deliver quantifiable effects on education success hence proving their effectiveness for improving education access in underprivileged regions.

The AI model based on differentials achieved AUC of 0.84 by using a privacy budget (epsilon) of 1.2 on the validation set. These findings imply positive trade-off between data confidentiality and accuracy of predicting the data. The results were calculated by precision and recall scores that were greater (more than) 80 %. The privacy-preserving technique resulted in only 5.6 percent performance drop in comparison with a non-private baseline model (AUC = 0.895), which can be deemed as acceptable in the educational application context focusing on ethical data privacy.

4.7. Interpretation of Results and Practical Implications

The research findings create substantial operational effects for educational policies while affecting how AI technology should be implemented in academic institutions. The experimental group's substantial learning advances prove that artificial intelligence tools assist in closing educational gaps that affect under-sourced educational environments. Institutions using education platforms and schools have the chance to personalize learning pathways through these technologies by establishing data privacy protocols to keep student information secure. Practitioners together with policymakers should understand that AI-driven learning tools need integration into the educational system because of research findings. Education should also focus on implementing coordinated data privacy solutions to achieve both security and effectiveness in AI systems.

More so, this framework positions applications by deploying it using modular architectures that support minimal hardware to meet these needs. To improve equity and accessibility, federated learning practices that are offline-compatible and open-source libraries of privacy-preserving techniques (e.g. PySyft, TenSEAL) should be used. These tools allow using simple devices like tablets and mobile phones to undergo privacy-preserving AI training without an internet connection. Notably, any technical implementation must be recognized until capacity-building programs are made available to the local educators and system administrators to support the sustainability of the adoption effort, more so when there is low IT literacy.

4.8. Limitations of the Study

Multiple constraints should be noted because of the study's promising results. The research used a small participant group within a restricted geographical area. The research findings need thorough verification through studies with big diverse groups in various educational settings.

Investigations concerning the privacy-preserving AI model show positive outcomes regarding cognitive learning yet have not yet determined its extended effects on students' academic performance or enrollment rates. Future research needs to establish the duration of these improvements through time.

4.9. Areas for Future Research

Research should study the implementation potential of AI-based teaching systems across different education settings especially those environments lacking proper technological systems. Studies must investigate both the ethical concerns of artificial intelligence use in education such as bias and fairness as well as transparency aspects.

Future research should also investigate how artificial intelligence models incorporating human feedback alongside machine learning capabilities can develop tailor-made adaptive educational experiences. This will help to diminish the shortcomings that emerge from complete AI automation so students can benefit from machine learning capabilities.

5. Conclusion, Summary, & Recommendations

5.1. Summary

This study was conducted to determine how privacy-preserving artificial intelligence models help students develop their cognitive skills on education platforms that use technology. Students' learning improvements and privacy preservation effectiveness were evaluated by conducting pre-tests and post-tests and implementing survey and interview methodologies. The research outcomes show that students who used the AI-based adaptive learning system achieved notable progress in their cognitive skills which extended to memory function together with problem-solving abilities and reasoning capabilities as well as analytical thinking abilities. Statistical analyses using paired-sample t-tests and regression analysis established the experimental group outperformed the control group especially in critical thinking and problem-solving cognitive areas.

Additionally, the study showed how AI-based adaptive learning systems can address knowledge inequalities through individualized education which respects privacy constraints. The statistical evidence confirms the value of these systems since they help educational institutions in areas requiring strict data protection. This research adds to existing scholarly works that explore AI education technologies while specifying the requirement of privacy-protection features.

5.2. Conclusion

The central research question addressed in this study was: *Can the implementation of AI-powered, privacy-preserving learning systems significantly improve cognitive skill development among students, particularly in underserved regions?* The findings of this study affirm that privacy-preserving AI systems can enhance cognitive outcomes by offering personalized learning opportunities that foster critical skills such as reasoning, problem-solving, and analytical thinking.

The hypothesis that the implementation of AI would lead to significantly improved cognitive outcomes in students, particularly in the experimental group, was supported by the results. Students exposed to the adaptive AI system exhibited substantial improvements in their cognitive skills, with a statistically significant difference between the experimental and control groups. This study underscores the potential for AI to revolutionize the way education is delivered, particularly in low-resource settings, where traditional methods of teaching and learning often fall short.

In light of these findings, the study contributes to both academic research and practical applications in the field of educational technology. It highlights the critical role of AI in driving educational equity, especially in contexts where privacy concerns can be a major barrier to the adoption of these technologies. Furthermore, this study lays the groundwork for future research in integrating privacy-preserving technologies into adaptive learning systems, making them not only more effective but also ethically sounds.

5.3. Recommendations

Based on the findings of this study, several recommendations can be made for educators, policymakers, and technology developers:

- **Expansion of AI-Driven Learning Systems:** Policymakers and educational stakeholders should consider expanding the use of AI-driven learning systems in schools, particularly in underserved and resource-constrained regions. These systems offer the potential to level the playing field, ensuring that all students have access to personalized, high-quality learning experiences.
- **Integration of Privacy Measures:** As privacy concerns continue to grow, educational technology developers must prioritize incorporating privacy-preserving AI technologies into their platforms. This could include the use of secure data storage systems, anonymization techniques, and differential privacy measures to ensure the protection of sensitive student data.
- **Long-Term Studies on Sustainability:** Future research should focus on the long-term impacts of privacy-preserving AI systems in education. Studies should examine whether the improvements in cognitive skills observed in this study are sustained over time and whether these systems can contribute to overall academic success.
- **Ethical Frameworks for AI in Education:** Ethical guidelines and frameworks for AI in education needs to be further developed. This includes addressing potential biases in AI algorithms, ensuring transparency in how AI models make decisions, and creating mechanisms for accountability in AI-powered educational tools.
- **Cross-National Collaboration:** Given the global nature of the digital divide in education, international collaborations should be encouraged to develop privacy-preserving AI solutions that can adapt to various cultural and socioeconomic contexts. This could help ensure that AI technologies are deployed ethically and effectively across different regions.
- In high-infrastructure settings, the institutions are advised to deploy federated learning infrastructures promoted by secure multi-party computation and real-time encryption standards. Such arrangements will be able to utilize cloud-based orchestrates with advanced privacy requirement compliance.
- Conversely, in the case of less resourceful settings, privacy protection may start with taking the form of lightweight wrappers of differential privacy, offline data processing and community-wide retraining of models through open source toolkits. Offline learning environments like the Kolibri ecosystem have proved that decentralized, privacy-preserving data systems can be successful and can make a real difference even in underserved settings when high-bandwidth deployments are not an option.

5.4. Concluding Remarks

Past research shows how privacy-protected AI technology will transform educational environments throughout the future. Intelligent systems that deliver secure

individualized learning according to student needs help students in underserved areas develop their brain-related skills better. Educational technology development requires immediate emphasis on student information protection so high-quality adaptive learning continues with appropriate security measures for sensitive data. This study creates a basis for future investigations about AI-related privacy concerns and education system enhancement which provide essential knowledge to utilize these technologies for improving educational equity and excellence.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Zhou, L., Li, F., Wu, S. and Zhou, M. (2020) "School's out, But Class's on", the Largest Online Education in the World Today: Taking China's Practical Exploration during the COVID-19 Epidemic Prevention and Control as an Example. *Best Evidence of Chinese Education*, **4**, 501-519. https://doi.org/10.15354/bece.20.ar023

[2] Feiner, L. (2020) ProctorU Confirms Data Breach Affecting Hundreds of Thousands of Students. CNBC. https://www.cnbc.com

[3] UNESCO (2021) Reimagining Our Futures Together: A New Social Contract for Education. https://unesdoc.unesco.org

[4] Holstein, K., McLaren, B.M. and Aleven, V. (2020) Student Privacy in AI-Enhanced Learning Environments. *AIED Conference Proceedings*, Chicago, 25-29 June 2019, 157-171.

[5] Chen, S.N.A., *et al.* (2023) AI-Driven Adaptive Learning Systems. *Nanotechnology Perceptions*, **20**, 3952-3960.

[6] Holstein, K. and Doroudi, S. (2021) Equity and Artificial Intelligence in Education: Will "AIEd" Amplify or Alleviate Inequities?

[7] Baxter, G. and Sommerville, I. (2011) Socio-Technical Systems: From Design Methods to Systems Engineering. *Interacting with Computers*, **23**, 4-17. https://doi.org/10.1016/j.intcom.2010.07.003

[8] Williamson, B. and Eynon, R. (2020) Historical Threads, Missing Links, and Future Directions in AI in Education. *Learning, Media and Technology*, **45**, 223-235. https://doi.org/10.1080/17439884.2020.1798995

[9] Zawacki-Richter, O., Marín, V.I., Bond, M. and Gouverneur, F. (2019) Systematic Review of Research on Artificial Intelligence Applications in Higher Education—Where Are the Educators? *International Journal of Educational Technology in Higher Education*, **16**, 1-27. https://doi.org/10.1186/s41239-019-0171-0

[10] Shneiderman, B. (2022) Human-Centered AI. Oxford University Press. https://doi.org/10.1145/3538882.3542790

[11] Robert, J. (2022) Student Data Privacy and Security: A Call for Transparent Practices. https://www.educause.edu/ecar/research-publications/2022/student-data-privacy-and-security-a-call-for-transparent-practices/introduction-and-key-findings

[12] Sari, H.E., Tumanggor, B. and Efron, D. (2024) Improving Educational Outcomes through Adaptive Learning Systems Using AI. *International Transactions on Artificial Intelligence* (*ITALIC*), **3**, 21-31. https://doi.org/10.33050/italic.v3i1.647

[13] Dönmez, E. (2024) The Future of Education: AI-Supported Reforms in the USA and

China. In: Akgün, B., Alpaydın, Y., Eds., *Global Agendas and Education Reforms*. Maarif Global Education Series, Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-97-3068-1_7

[14] Henkel, O., *et al.* (2024) Effective and Scalable Math Support: Evidence on the Impact of an AI-Tutor on Math Achievement in Ghana. https://arxiv.org/abs/2402.09809

[15] Apple (2025) Differential Privacy. https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf

[16] GDPR.eu (2023) Understanding GDPR for Education Providers. https://gdpr.eu

[17] UNESCO (2021) Reimagining Our Futures Together.

[18] Ng, A. and Pasinetti, A. (2025) Kira Learning: Redefining Teaching with AI Agents. Business Insider. https://www.businessinsider.com

[19] Creswell, J.W. and Plano Clark, V.L. (2018) Designing and Conducting Mixed Methods Research. 3rd Edition, Sage Publications.

[20] Abadi, M., Chu, A., Goodfellow, I., McMahan, H.B., Mironov, I., Talwar, K., *et al.* (2016) Deep Learning with Differential Privacy. *Proceedings of the* 2016 *ACM SIGSAC Conference on Computer and Communications Security*, Vienna, 24-28 October 2016, 308-318. https://doi.org/10.1145/2976749.2978318

[21] Braun, V. and Clarke, V. (2006) Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, **3**, 77-101. https://doi.org/10.1191/1478088706qp063oa

[22] Van Lehn, K. (2011) The Relative Effectiveness of Human Tutoring, Intelligent Tutoring Systems, and Other Tutoring Systems. *Educational Psychologist*, **46**, 197-221. https://doi.org/10.1080/00461520.2011.611369

[23] USA Department of Education (2022) Artificial Intelligence and the Future of Teaching and Learning. https://www.ed.gov/sites/ed/files/documents/ai-report/ai-report.pdf

Appendix

Appendix 1: Semi-Structured Interview Questions for Teachers and Administrators Using EdTech Systems

Objective: Understand teachers' and administrators' experiences, challenges, and perceptions regarding AI-powered EdTech platforms, with a focus on privacy and data security.

1) General Experience with EdTech Systems

- Can you describe your experience with the EdTech systems currently used in your institution? How do they fit into your daily operations and teaching routines?
- How would you rate the overall effectiveness of these systems in supporting student learning outcomes?

2) Perception of Data Security and Privacy

- Are you aware of how student data is being collected and stored within the EdTech systems?
- Do you believe the platform ensures the privacy and security of student data? Why or why not?
- Have there been any instances or concerns regarding data breaches or privacy issues in your experience with EdTech systems?

3) AI and Data Usage in Educational Platforms

- How do you feel about the use of AI algorithms in making decisions related to students' performance and learning?
- Do you trust the AI system to maintain student privacy while delivering educational content or assessments?
- In your opinion, what kind of safeguards should be in place to protect student data while using AI in EdTech platforms?

4) Engagement with Privacy-Enhanced Systems

- Have you encountered any privacy-enhanced EdTech platforms or tools? If so, what were your impressions?
- What would make you more willing to use or adopt AI-driven, privacy-preserving EdTech systems in your institution?

5) Challenges and Recommendations

- What are the biggest challenges you have faced in terms of data privacy and security when using EdTech systems?
- What improvements or features would you suggest to ensure more robust data privacy protection within AI-enhanced EdTech systems?

Appendix 2: Semi-Structured Interview Questions for AI Developers and EdTech Platform Designers

Objective: Gather insights from AI developers and platform designers about the technical and ethical considerations of privacy-preserving AI models in EdTech.

1) Design and Development of EdTech AI Systems

- Can you describe the design and development process for the AI models used

in your EdTech platform?

- How do you ensure that the AI systems you develop are effective and adhere to privacy protection principles?

2) Privacy Considerations in AI Model Design

- What measures are integrated into your AI systems to safeguard student data privacy? Can you explain how these privacy measures are embedded into the system's architecture?
- How do you balance the need for personalized learning with data privacy concerns?
- What frameworks (e.g., Differential Privacy, Federated Learning) do you use to minimize privacy risks?

3) Legal and Regulatory Compliance

- How do you ensure that your platform complies with data privacy regulations such as the GDPR (General Data Protection Regulation) or CCPA (California Consumer Privacy Act)?
- What steps are taken to prevent the misuse of personal data within AI-driven educational platforms?

4) Challenges and Solutions

- What are some of the biggest challenges you face when implementing privacy-preserving AI models in education?
- How do you handle the ethical dilemmas related to student data, especially when dealing with sensitive or identifiable information?

5) Future of Privacy-Preserving AI in EdTech

- How do you see the future of privacy-preserving AI in educational technology evolving? Are there any emerging technologies that could enhance privacy protections?
- In your opinion, what are the critical improvements needed in current AI-based EdTech systems to ensure robust data privacy for students?

Appendix 3: Semi-Structured Interview Questions for Policy Experts in Data Privacy

Objective: Understand policy perspectives on data privacy issues within AI-driven EdTech platforms.

1) Current Privacy Regulations in EdTech

- What are the primary privacy regulations that EdTech platforms need to follow? Are there any differences in how these regulations are applied across different regions (e.g., EU vs. USA)?
- Do you think current regulations are adequate in protecting student data within AI-enhanced learning environments?

2) Policy Challenges

- What challenges do policymakers face in ensuring data privacy in the context of AI and EdTech systems?
- How can governments ensure that EdTech companies remain compliant with privacy laws while also innovating with AI technology?

3) Data Sovereignty and Global Perspectives

- How do data sovereignty issues (i.e., where data is stored and processed) impact the privacy of students, especially in a globalized education landscape?
- Do you see disparities in data privacy protection between the Global South and other regions? How can these differences be addressed?

4) The Role of AI in Privacy Protection

- How can AI technologies be integrated into policy frameworks to improve data privacy protections, while still enabling effective learning?
- What role do you see for emerging technologies like Federated Learning or Differential Privacy in shaping future policies for EdTech systems?

5) Recommendations for Policy Improvement

- What policy recommendations would you make to ensure that the use of AI in education does not compromise student data privacy?
- How can governments and educational institutions work together to create more robust privacy standards for EdTech systems?

Appendix 4: User Survey on Perceptions of Data Security and Fairness

Objective: Measure user perceptions regarding data security and fairness of AI-powered EdTech systems.

Part 1: General Information

1) Age: _____

2) Role:

- □Student
- □Teacher
- □Administrator
- □Parent

Part 2: Data Security Perception

1) How concerned are you about the security of your personal data when using AI-powered EdTech systems?

- □Very concerned
- □Somewhat concerned
- □Neutral
- □Not concerned

2) Do you believe that the EdTech platforms you use protect your data adequately?

- □Yes
- □No
- □Unsure

3) Have you experienced or heard about data breaches or privacy incidents related to EdTech platforms?

- □Yes
- □No

Part 3: Fairness Perception

1) Do you think AI systems in EdTech platforms treat all students equally?

- □Yes
- □No
- □Unsure

2) In your opinion, do AI-powered systems in education have the potential to introduce bias or unfair treatment?

- □Yes
- □No
- □Unsure

Part 4: Willingness to Engage with Privacy-Enhanced Systems

1) Would you be more likely to use an EdTech platform that prioritizes data privacy (e.g., uses privacy-preserving AI techniques like Differential Privacy)?

- □Yes
- □No
- □Maybe

2) What features would increase your trust in the privacy of an EdTech system? (Select all that apply)

- □Clear privacy policies
- □Transparency about data usage
- □User control over personal data
- □Third-party audits or certifications