DATA STORAGE AND PRIVACY IN AI SYSTEMS FOR RISK IDENTIFICATION AND PERSONALIZED INTERVENTIONS IN SPECIAL EDUCATION

Shakhnoza Khaydarova

PhD Student at Lincoln University, California, USA

Abstract: Artificial Intelligence (AI) has transformed education, especially in identifying risks of disabilities and recommending personalized treatments and Individualized Education Programs (IEPs) for students with learning disabilities. While the potential of AI in special education is immense, challenges surrounding data storage and privacy pose significant concerns. This article explores the intersection of AI-driven educational technologies, data privacy regulations, and secure data storage solutions, offering insights into ethical frameworks and best practices to mitigate privacy risks while maximizing the benefits of AI.

Key words: AI in special education, data storage, privacy, IEP, personalized treatment, ethical AI

Аннотация: Искусственный интеллект (ИИ) произвел революцию в образовании, особенно в выявлении рисков инвалидности и создании персонализированных планов лечения и ИПР (индивидуальных программ развития) для учащихся с особыми образовательными потребностями. Несмотря на огромный потенциал технологий ИИ в специальном образовании, проблемы, связанные с хранением данных и конфиденциальностью, вызывают серьезные опасения. В данной статье рассматриваются пересечения технологий ИИ в образовании, нормативных актов по защите данных и решений для безопасного хранения данных. Также предлагаются этические рамки и лучшие практики для минимизации рисков конфиденциальности при максимальном использовании преимуществ ИИ.

Ключевые слова: ИИ в специальном образовании, хранение данных, конфиденциальность, ИПР, персонализированное лечение, этический ИИ

Annotatsiya: Sun’iy intellekt (SI) ta’limni, xususan, o’rganishda qiyinchilik yoki oqsashni aniqlash va o‘quvchilarning o‘ziga xos ehtiyojlari uchun shaxsiylashtirilgan davolash hamda IO’D (individuallashtirilgan o‘quv dasturi) tavsiyalarini yaratishni o‘zgartirdi. Maxsus ta’limda SI texnologiyalarining potentsiali katta bo‘lsa-da, ma’lumotlarni saqlash va maxfiylik bilan bog‘liq muammolar jiddiy xavotir uyg‘otadi. Ushbu maqola ta’limdagi sun’iy intellekt texnologiyalari, ma’lumotlarni maxfiy saqlash bo‘yicha qoidalarga rioya qilish va xavfsiz saqlash usullari haqida so‘z yuritadi. Shuningdek, maxfiylik xavfini kamaytirish va SI foydasini oshirish uchun axloqiy asoslar va eng yaxshi tajribalar tahlil qilinadi.

Kalit so‘zlar: Sun’iy intellekt maxsus ta’limda, ma’lumotlarni saqlash, maxfiylik, SHD, shaxsiylashtirilgan davolash, sun’iy intellekt

Introduction

The integration of AI in education has led to groundbreaking advancements in diagnosing learning disabilities, tracking student progress, and creating adaptive learning systems tailored to individual needs. AI models analyze data to predict potential risks of disabilities and suggest personalized treatment plans or IEPs for students. However, this reliance on large volumes of sensitive data raises critical questions about data security, storage, and privacy, particularly given the legal and ethical responsibilities of educational institutions. This article examines the implications of data storage and privacy in AI-driven educational technologies, explores ethical frameworks, and suggests research-based best practices for secure data management. It incorporates research methods such as surveys, case studies, and data analysis, and provides recommendations for addressing privacy risks while enhancing the effectiveness of AI solutions.

AI in Special Education

AI systems process sensitive data such as academic performance, behavioral assessments, and medical records to make predictions and recommendations. AI technologies in special education can be categorized according to their several purposes:

1. Risk Identification: Algorithms analyze behavioral patterns, academic performance, and neurodevelopmental assessments to detect early signs of learning disabilities.
2. Personalized Treatment Plans: AI suggests tailored interventions based on the unique needs of students.
3. Automated IEP Recommendations: AI-powered tools streamline the creation and revision of IEPs by suggesting goals, accommodations, and progress monitoring strategies.

While we use AI to get personalized and best tailored plan process requires the collection of a variety of personal data, including:

- Academic records
- Behavioral assessments
- Psychometric tests
- Medical and psychological histories

While these tools provide significant benefits, they also raise concerns about data security, privacy, and compliance with legal standards.Detailed explanation of risks introduces threats such as:

1. Data Breaches: Unauthorized access to sensitive student data could lead to identity theft or misuse.

2. Lack of Consent: Collecting data without informed parental or guardian consent violates ethical and legal standards.

3. Algorithmic Bias: Improper data handling can exacerbate biases, resulting in inequitable outcomes for students.

Discussion of Research Literature on the risks and regulatory frameworks of AI systems' and AI tools for Special Education highlights the challenges, advancements, and best practices in this domain.

1.1 The Sensitivity of Data in Special Education

Special education data encompasses sensitive information, such as health records, behavioral patterns, and individualized learning plans. Researchers like Johnson et al. (2022) have emphasized that such data requires heightened protection to prevent breaches and ensure compliance with laws such as FERPA and GDPR. They argue that the complexity of managing such data is compounded by the need for real-time AI processing, which exposes it to additional vulnerabilities.

1.2 Ethical Dilemmas in Data Usage

Literature by Binns and Veale (2020) explores ethical concerns about the use of sensitive data in AI systems. The authors highlight that while AI can improve educational outcomes, its deployment often lacks sufficient stakeholder consultation, leading to potential misuse of data or lack of informed consent from parents.

1.3 Algorithmic Bias and Security Risks

Raji et al. (2021) draw attention to how biased data sets in AI systems not only lead to discriminatory outcomes but also create additional risks when data is mishandled. They point out that bias and security issues are interconnected, as poorly managed data sets are more likely to be exploited or compromised.

Research Methods

This study used a combination of methods to investigate data security challenges in special education AI:

- Case Studies: We analyzed three AI-driven educational tools to evaluate their data security practices.

And conducted surveys among 150 educators to assess awareness of data security risks.

- Secondary Research: Reviewed literature on data breaches and AI ethics in education.

4. Findings

After surveys and interviews following key risks were identified related to data security in AI for special education:

- Unauthorized Access: Weak access controls allow unauthorized personnel to view or misuse sensitive data.
- Inadequate Encryption: Lack of encryption leaves data vulnerable during storage and transmission.
- Data Anonymization Issues: Poor anonymization practices can still allow identification of students.

Research shows that by advancing following measures are recommended:

2.1 Data Encryption and Anonymization

Encryption and anonymization are widely acknowledged as effective security practices. Rizvi and Kumar (2023) discuss how these techniques ensure data privacy without compromising AI functionality. Federated learning—a method that processes data locally without transferring it to centralized servers—has emerged as a promising solution.

2.2 Privacy-Preserving AI Models

Chen and Zhang (2023) highlight advancements in privacy-preserving AI models that allow for data analysis while protecting individual identities. Differential privacy, for instance, introduces statistical noise into datasets, making it difficult to trace data back to specific individuals.

2.3 Blockchain Technology in Education

Blockchain technology has been proposed as a secure alternative for managing sensitive educational data. A study by Grech and Camilleri (2020) demonstrates how blockchain can provide transparent yet secure record-keeping for AI systems, significantly reducing the risk of unauthorized access.

3. Regulatory Frameworks and Compliance

3.1 FERPA and GDPR

The Family Educational Rights and Privacy Act (FERPA) and the General Data Protection Regulation (GDPR) provide foundational frameworks for data security. Researchers like Shibani et al. (2022) argue that while these regulations are robust, many AI tools in education fail to comply fully due to poor implementation practices.

3.2 Emerging Standards in AI Ethics

The European Commission’s Ethics Guidelines for Trustworthy AI (2019) outline principles for transparency, accountability, and data privacy. These guidelines have been influential in shaping policies for educational AI systems, but their adoption remains inconsistent across regions.

4. Best Practices in Secure AI Deployment

4.1 Stakeholder Involvement

Studies by Holmes et al. (2023) emphasize the importance of involving educators, parents, and students in the development and deployment of AI systems. This collaborative approach ensures that ethical and security concerns are addressed early in the design phase.

4.2 Continuous Auditing and Monitoring

Johnson et al. (2022) propose regular audits of AI systems to identify and mitigate potential vulnerabilities. These audits should be complemented by continuous monitoring to detect unauthorized access or data breaches in real time.To ensure compliance with data privacy laws, educational institutions leveraging AI must adhere to regulations such as:

- Family Educational Rights and Privacy Act (FERPA): Governs access to student education records in the U.S.
- General Data Protection Regulation (GDPR): Ensures the rights of individuals to control their personal data within the European Union.
- Children’s Online Privacy Protection Act (COPPA): Protects children under 13 by regulating the collection of their data online.

These frameworks require transparency, accountability, and secure storage mechanisms for managing data.

Conclusion

The existing body of research underscores the importance of data security in AI applications for special education. While advancements in encryption, federated learning, and privacy-preserving models show promise, challenges related to ethical data usage, compliance, and stakeholder involvement persist. Addressing these issues requires a multidisciplinary approach that combines technical innovation, regulatory oversight, and active stakeholder participation.

References:

1. Binns, R., & Veale, M. (2020). “Data ethics and governance in education: Challenges and opportunities.” AI & Society, 35(3), 567-580.

2. Chen, J., & Zhang, Y. (2023). “Ethical Challenges in AI-Driven Education” Journal of Educational Technology, 45(3), 215-230.

3. European Commission. (2019). Ethics Guidelines for Trustworthy AI: Retrieved from https://ec.europa.eu

4. Grech, A., & Camilleri, A. F. (2020). “Blockchain in Education: Opportunities and Challenges.” European Journal of Education, 55(3), 402-418.

5. Holmes, W., et al. (2023). “Engaging Stakeholders in AI Development for Education” Computers in Human Behavior, 135, 107569

6. Johnson, L., et al. (2022). “AI and Data Privacy in Education: An Empirical Study.” Computers & Education, 181, 104437

7. Raji, I. D., et al. (2021). “Algorithmic Bias in Education: Risks and Solutions.” Proceedings of the National Academy of Sciences, 118(15), e2022044118

8. Rizvi, S., & Kumar, P. (2023). “Federated Learning in AI Applications: A Privacy-Preserving Approach.” AI & Society, 38(2), 157-169.

9. Shibani, A., et al. (2022). “Compliance with Data Privacy Regulations in Educational AI Systems” Journal of Learning Analytics, 9(1), 78-95.