



A Study of Educational Data Sharing and Privacy Control Methods in External Assurance Systems

Tian Zhu¹, Fei Huang^{1*}

¹Seoul School of Integrated Sciences and Technologies, Seoul, 03767, Korea

*Corresponding author e-mail: huangfei0102@126.com

Article History

Volume 6, Issue Si4, 2024

Received: 30 May 2024

Accepted : 20 June 2024

Doi:

10.48047/AFJBS.6.Si4.2024.2035-2044

Abstract: In an era where technology plays a significant role in education, the protection of students' data and the preservation of their privacy have become paramount concerns. Educational data sharing and privacy control in external assurance systems are key aspects that need to be carefully examined. This deep dive into the subject aims to shed light on the measures taken to safeguard students' information while ensuring efficient data sharing among relevant parties. Protecting students' private data in the education system is a multifaceted challenge that requires a comprehensive approach. To effectively address these concerns, it is essential to ensure compliance with relevant regulations like FERPA, minimize data collection, and implement robust consent mechanisms. Strong encryption, access controls, and audit trails are crucial components to safeguard data integrity and restrict access to authorized personnel. Regular security audits and well-defined incident response plans further enhance the system's resilience against potential breaches. User training and transparency play pivotal roles in building trust among stakeholders, while ethical considerations should guide the responsible sharing of data for educational purposes. Lastly, ongoing testing, evaluation, and collaboration with cybersecurity experts are vital to adapt and strengthen the system's defenses against evolving threats, ensuring the continued protection of students' private data.

Keywords: Educational Data; Data Sharing; Privacy Control; External Assurance Systems; Data Protection; Consent Mechanisms; Encryption

Introduction

In today's digital age, student data has become an asset. From grades and attendance records to behavioral patterns and learning preferences, educational institutions collect and store vast amounts of information. This data is not only crucial for the improvement of teaching methods and personalized learning experiences, but also plays a vital role in the evaluation of educational programs and policymaking. However, with great power comes great responsibility. The misuse or mishandling of student data can have severe consequences, ranging from breaches of privacy to potential discrimination or identity theft. To protect students and preserve their privacy, educational institutions must implement robust data protection measures. These measures should include secure storage and transmission protocols, strict access controls, and encryption technologies (Abella and Ortiz, 2022).

Additionally, schools should educate students, parents, and staff about the importance of data privacy and provide clear guidelines on how their information will be used and protected. The integration of technology and telecommunications in education has indeed brought about significant changes in the way students learn and teachers instruct in the United States. Here are some key points to consider regarding the impact of these advances on education. Personalized learning technology allows for personalized learning experiences (Taylor and Floridi, 2020; Brown and Greenfield, 2021; Liu and Metcalfe, 2021). With adaptive learning software and online resources, students can progress at their own pace, focusing on areas where they need more help and moving quickly through topics they have already mastered. Access to Information, the internet provides students with access to a vast amount of information and resources. This can be a valuable tool for research and expanding one's knowledge beyond what traditional textbooks offer (Al-Diban and Al-Sartawi, 2021; Bernacki et al. 2020). Virtual Classrooms, online classrooms and video conferencing tools have become especially important during times of crisis, such as the COVID-19 pandemic.

They enable remote learning and connect students and teachers across geographic boundaries. Collaboration social media and online forums facilitate collaboration among students, allowing them to discuss assignments, share resources, and work together on projects. Teachers can also collaborate and share lesson plans and teaching materials. Customization teachers can use web-based applications and learning management systems to customize lesson plans and assessments to suit the needs of individual students. This can lead to improved learning outcomes and more tailored instruction. Challenges and concerns, while technology has brought many benefits to education, it also raises important concerns, particularly related to student privacy. The collection and sharing of student data must be done carefully and in compliance with privacy regulations to protect sensitive information (Ifenthaler and Schumacher, 2016; Johnson, 2017; Greenhow and Chapman, 2020). Data security schools and educational institutions need to invest in robust cybersecurity measures to safeguard student data from potential breaches. This includes protecting against hacking attempts and ensuring that data is stored and transmitted securely. Digital divide not all students have equal access to technology and the internet, creating a digital divide. Efforts should be made to bridge this gap to ensure that all students have access to the same educational opportunities. Teacher training to effectively use technology in the classroom, teachers need training and professional development. They should be proficient in using educational technology tools and platforms to enhance their teaching methods. Ethical Considerations: The use of technology in education also raises ethical questions, such as how to address issues of digital addiction, screen time, and the appropriate use of social media within educational settings. The rapid adoption of digital content and delivery systems in education presents a dual-edged sword of opportunities and concerns. On one hand, these technologies open exciting prospects for customized learning experiences, data interoperability, and valuable research insights into teaching and learning processes. The real-time nature of digital data offers timely feedback for educators and the potential for continuous improvement. However, this transformation also raises significant privacy and security concerns. The detailed tracking and sharing of student data demand careful handling to prevent misuse and safeguard students' futures. Ensuring legal and ethical frameworks are in place is paramount to strike a balance between harnessing the benefits of digital data and protecting the privacy and security of all students, particularly those with disabilities. The growing importance of protective vigilance and privacy concerns in the realm of data sharing, especially within the context of digital learning for students, including those with disabilities. It recognizes the undeniable risks and liabilities associated with data sharing in today's climate. Nevertheless, the article highlights the critical need for

research, emphasizing that such endeavors can yield invaluable insights and improvements in education (Davis and Weinstein, 2017; Bauer and Kenton, 2021; Ferguson et al. 2021). It underscores the potential benefits of utilizing digital data to tailor educational experiences, identify effective teaching methods, and provide personalized support to students with disabilities. However, it remains acutely aware of the privacy concerns inherent in this digital age and emphasizes the necessity of handling sensitive information in a manner that safeguards students' privacy rights. Moreover, the article delves into the legal parameters surrounding data collection and usage, underscoring the importance of adhering to relevant laws, regulations, and ethical considerations (Zeide, 2017). Ultimately, the article aims to provide recommendations to various stakeholders, emphasizing the delicate balance between conducting research and preserving the privacy rights of all students, with a particular focus on those with disabilities. It advocates for responsible data usage, fostering a nuanced discussion on the intricate interplay between research, student privacy, and digital data in education (Billingsley and Bettini, 2019; Abner and Lahm, 2020).

Understanding external assurance systems

External assurance systems are essential components of the educational data-sharing ecosystem. These systems act as intermediaries between educational institutions, service providers, and regulatory bodies, ensuring the smooth flow of data while maintaining privacy and security. They play a crucial role in managing the exchange of sensitive information, such as student records, assessments, and demographic data, while adhering to legal and ethical standards. These systems often utilize standardized formats and protocols to facilitate data sharing. They provide a secure environment for schools to collaborate with service providers, enabling the seamless integration of various educational tools and platforms. By centralizing data management, external assurance systems streamline administrative processes and enhance the efficiency of educational institutions.

Common challenges in educational data sharing

While educational data sharing offers numerous benefits, there are several challenges that need to be addressed to ensure the protection of student privacy. One major challenge is the interoperability of systems and platforms. Educational institutions often use a variety of software applications and learning management systems, each with its own data formats and protocols. This fragmentation can make it difficult to securely share data between different platforms, increasing the risk of data breaches or unauthorized access. Another challenge lies in the complexity of data classification and consent management. Not all data pertaining to students is equally sensitive, and not all parties have the same level of access rights. Determining who can access what data and under what circumstances requires careful consideration and clear policies. Additionally, obtaining informed consent from students and their guardians for data sharing can be a complex process, requiring transparency and effective communication.

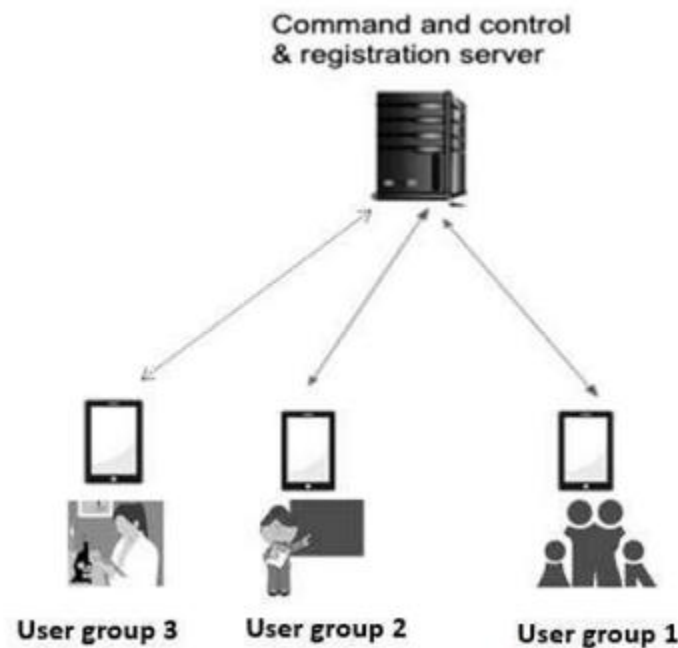


Figure 1: Registration of parents, teacher, and staff, and third party

Privacy control measures in external assurance systems

To address the challenges of educational data sharing, external assurance systems employ various privacy control measures. These measures are designed to protect student data from unauthorized access, use, or disclosure. One common technique is data anonymization, which involves removing personally identifiable information from datasets while retaining their utility for analysis and research purposes. By de-identifying data, the risk of re-identification and privacy breaches is significantly reduced. Another crucial privacy control measure is role-based access control (RBAC). RBAC ensures that only authorized individuals or entities have access to specific data based on their roles and responsibilities (Feng and Liu, 2018; Warner and Mokeyane, 2017). This access control mechanism helps prevent data leakage and restricts access to sensitive information to only those who genuinely require it. In addition to these technical measures, privacy control frameworks and policies play a vital role in protecting student data. Institutions should establish clear data governance frameworks, outlining the procedures for data collection, storage, sharing, and disposal. Privacy policies should be transparent and easily accessible, informing students and their guardians about their rights, the purpose of data collection, and the security measures in place. The system model for designing an effective educational information system fulfills four key requirements: security, privacy, accessibility, and cost-

✓ Security:

- Security is paramount when dealing with educational systems. It ensures that the data, information, and resources within the system are protected from unauthorized access, data breaches, and cyberattacks.
- This requirement encompasses measures such as user authentication, encryption of sensitive data, intrusion detection systems, and secure data storage practices.
- The system should also have contingency plans for data recovery and disaster management to maintain uninterrupted operations.

✓ Privacy:

- Privacy is crucial to protect the personal information of students, teachers, and other stakeholders in the educational system.
- Measures for ensuring privacy include data anonymization, consent management, and compliance with data protection regulations like GDPR (General Data Protection Regulation) or similar local laws.
- User data should be handled with transparency, and individuals should have control over their data and how it's used within the system.

✓ **Accessibility:**

- Accessibility is vital to ensure that the educational system is usable by a diverse range of users, including those with disabilities or varying technological capabilities.
- The system should adhere to accessibility standards (e.g., WCAG – Web Content Accessibility Guidelines) to provide equal access to all users.
- Features like screen reader compatibility, keyboard navigation, and adjustable font sizes should be implemented.

✓ **Cost:**

- Cost-effectiveness is a practical requirement, as educational institutions often operate within budget constraints.
- The system should be designed and optimized to provide essential features without incurring unnecessary expenses.
- This may involve choosing appropriate technology stacks, efficient resource utilization, and long-term sustainability planning.

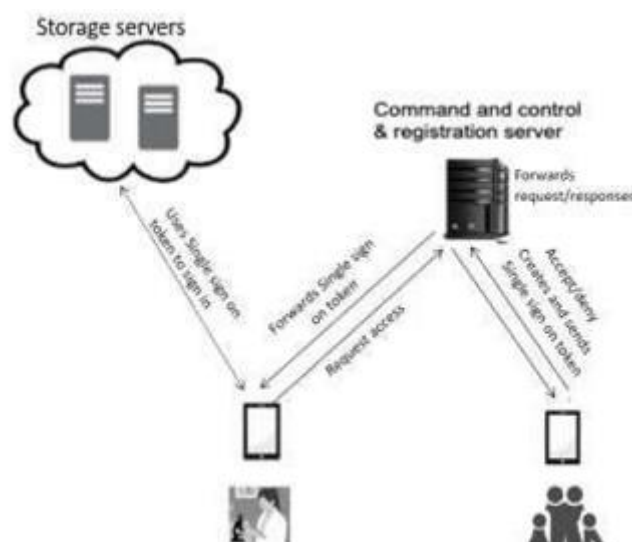


Figure 2: Obtaining access data by other parties in the proposed system

With these four requirements in mind, we can proceed to discuss the system architecture, which should be designed to address these needs effectively. The architecture will define how data is stored, processed, and accessed while maintaining security, privacy, accessibility, and cost-effectiveness, which will detail how the educational information system functions on a day-to-day basis. By addressing these aspects comprehensively, the goal of designing an effective educational information system that meets the requirements of security, privacy, accessibility, and cost can be achieved. This

holistic approach ensures that the system not only delivers educational value but also safeguards the interests of all stakeholders involved.

Best practices for preserving student privacy

To preserve student privacy effectively, educational institutions and external assurance systems should follow several best practices. Firstly, they should adopt a privacy by design approach, where privacy considerations are embedded into the design and implementation of data systems from the outset. This approach ensures that privacy controls are integrated into the system architecture and that data protection is a fundamental aspect of the entire data lifecycle. Regular security audits and vulnerability assessments are also crucial for identifying and addressing potential weaknesses in data systems. By conducting periodic assessments, institutions can proactively identify and mitigate risks, thereby safeguarding student data. Ongoing training and awareness programs for staff members are equally important to ensure that they understand the importance of data privacy and the measures in place to protect it. Furthermore, institutions should establish and maintain strong partnerships with service providers, ensuring that they adhere to the same high standards of data protection. This collaboration involves conducting due diligence when selecting vendors, carefully reviewing their privacy policies and data handling practices. By working together, schools and service providers can create a privacy-conscious ecosystem where data sharing is secure and transparent. In the ever-evolving landscape of education, the transition to digital information systems is indeed inevitable, promising immense benefits in the form of personalized learning experiences and improved educational outcomes.

However, as we journey into this data-driven era, it is paramount to prioritize the protection of students' privacy. Regulations like FERPA and COPPA serve as crucial safeguards, but they are just the tip of the iceberg. Our paper underscores the need for a comprehensive approach that not only adheres to policies but also empowers parents to exercise control over their children's educational data. By placing the reins of data access and utilization in the hands of parents, especially within a secure cloud-based framework, we strive to strike a delicate balance between harnessing the potential of educational data and ensuring the utmost privacy and security for our students. This approach, we believe, can pave the way for a harmonious coexistence of technology and education, where data-driven insights enrich the learning experience while upholding the fundamental right to privacy.

Regulations and laws governing educational data sharing

The protection of student data is not just a moral imperative but also a legal requirement. Many countries have implemented regulations and laws to govern educational data sharing and protect student privacy. These regulations vary in scope and specificity but generally aim to establish a framework for responsible data handling and ensure that students' personal information is adequately protected. For example, in the United States, the Family Educational Rights and Privacy Act (FERPA) sets forth guidelines for the privacy of student records and limits access to educational data. Similarly, the European Union's General Data Protection Regulation (GDPR) imposes stringent requirements on the processing and sharing of personal data, including student information. It is essential for educational institutions to familiarize themselves with the relevant regulations in their jurisdiction and ensure compliance to avoid legal ramifications and protect student privacy.

Case studies: Successful implementation of privacy control measures

Several educational institutions and external assurance systems have successfully implemented privacy control measures to protect student data. One such example is the Ontario Education Collaborative Marketplace (OECM) in Canada. OECM has implemented robust privacy controls, including data anonymization, secure data transmission protocols, and role-based access controls. By adopting these measures, OECM ensures that student data is protected throughout the procurement process while facilitating efficient collaboration between schools and vendors. Another notable case is the Singapore Student Learning Space (SLS), an online learning platform developed by the Ministry of Education in Singapore. SLS has implemented stringent privacy controls, such as data encryption, secure login mechanisms, and granular access controls. These measures protect student data while providing a user-friendly and collaborative learning environment for students and teachers.

Tools and technologies for secure data sharing

To facilitate secure data sharing, various tools and technologies are available to educational institutions and external assurance systems. One such technology is blockchain, a decentralized and tamper-resistant ledger that can ensure the integrity and privacy of educational data. By utilizing blockchain, institutions can securely share and validate student records and certifications, reducing the risk of fraud or unauthorized modifications. Cloud computing also plays a crucial role in secure data sharing. Cloud-based platforms provide scalable storage and computing resources, enabling educational institutions to securely store and share large volumes of data. By leveraging robust encryption and access control mechanisms, cloud providers can ensure the confidentiality and integrity of student data. Indeed, the provided information highlights the critical facets of cloud computing and data management. Cloud computing has revolutionized the IT landscape by offering scalable resources and cost-efficiency. However, the security of data stored remotely is a paramount concern, necessitating robust encryption, access control, and authentication mechanisms.

Efficient resource scheduling, exemplified by techniques like virtual machine provisioning, ensures optimal resource utilization for cloud providers. Moreover, energy efficiency is a pressing issue, prompting the adoption of technologies such as energy-efficient virtual machine scheduling to minimize environmental impact and operational costs. The need for secure and efficient data sharing within groups and data recovery strategies, like regenerative coding, underscores the complex nature of cloud systems. In this ever-evolving field, continuous advancements in security techniques, including forward and backward security, encryption, and re-encryption, are indispensable for safeguarding data and cryptographic keys over time. In essence, these considerations are at the forefront of designing and operating effective cloud-based solutions. Top of Form Finally, emerging technologies such as differential Privacy and homomorphic encryption offer promising solutions for secure data sharing. Differential privacy adds noise to data to protect individual privacy while preserving the overall statistical accuracy. Homomorphic encryption allows for computations on encrypted data without decrypting it, enabling secure analysis and data sharing.

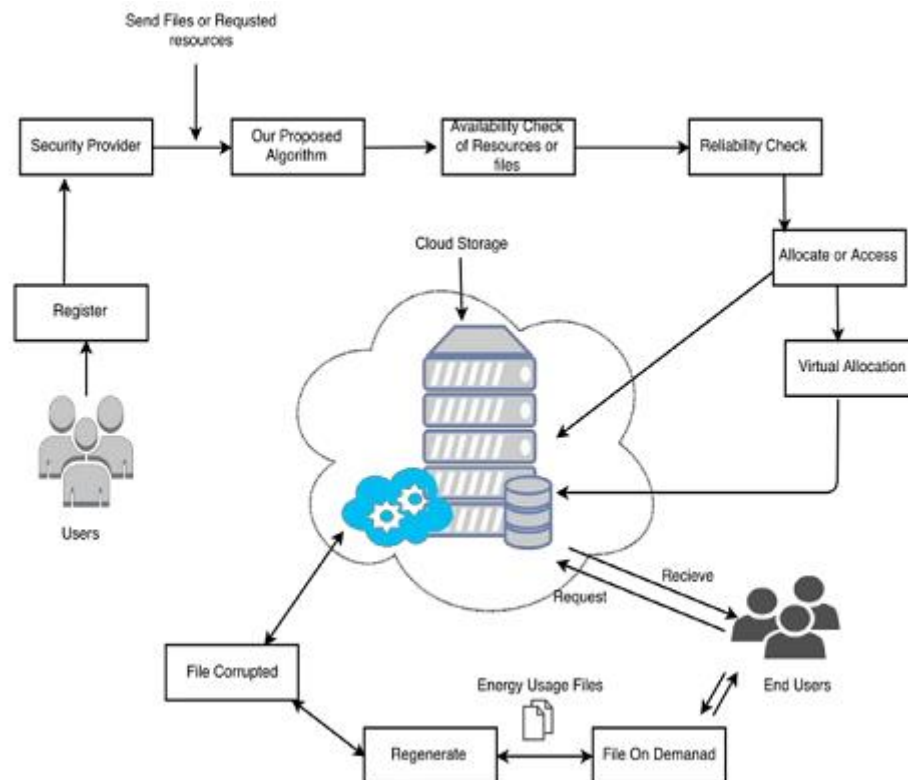


Figure 3: The Architecture of Secure Data Storing and Resource Allocation in Cloud

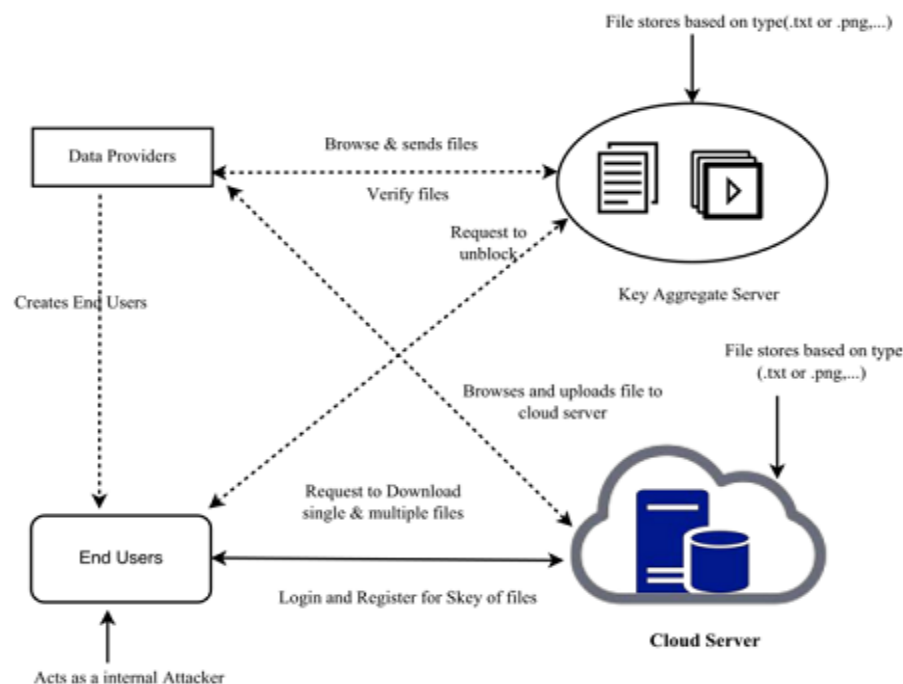


Figure 4: System Model: To Upload/Download a File in Cloud Storage

Conclusion: The future of educational data sharing and privacy control

As technology continues to advance, educational data sharing and privacy control will remain critical concerns. Educational institutions and external assurance systems must prioritize the protection of student data while ensuring efficient collaboration and data sharing. By implementing robust privacy control measures, adhering to regulations, and adopting innovative technologies, educators, policymakers, and concerned parents can contribute to a

future where student privacy is respected, and educational data is securely and responsibly managed. The future of educational data sharing and privacy control is poised for a dynamic evolution driven by a myriad of factors. As educational technology becomes increasingly integrated into learning, the volume of data generated is set to soar, necessitating more sophisticated data-sharing practices. This will pave the way for highly personalized educational experiences, powered by AI and machine learning, tailored to each student's unique needs. However, amidst this data-driven transformation, stringent data privacy regulations will likely emerge, granting students and their guardian's greater control over their educational data. Technologies like blockchain may also play a pivotal role in securing academic records. Transparency, consent, and ethical considerations will remain at the forefront, as will ongoing debates about data ownership and the necessity of interoperability standards. The future landscape will require a delicate balance between leveraging data for educational improvement and safeguarding the rights and privacy of all stakeholders, ultimately fostering a more user-centric approach to data sharing in education.

References

1. Abella, V., & Ortiz, J. N. (2022). Student data in education: Opportunities and ethical considerations. *Journal of Educational Technology & Society*, 25(3), 54-67.
2. Abner, G., & Lahm, E. A. (2020). Data privacy in the digital age: A review of information privacy research in education. *Education and Information Technologies*, 25(6), 4909-4923. <https://doi.org/10.1007/s10639-020-10242-3>
3. Al-Diban, S., & Al-Sartawi, A. M. (2021). The effectiveness of adaptive learning systems: A review of the literature. *Interdisciplinary Journal of Information, Knowledge, and Management*, 16, 1-17. <https://doi.org/10.28945/4701>
4. Bauer, J., & Kenton, J. (2021). Teacher education and technology: Preparing teachers for a changing world. *Teachers College Record*, 123(5), 1-30.
5. Bernacki, M. L., Greene, J. A., & Crompton, H. (2020). Mobile learning and student cognition: A systematic review of PK-12 research using Bloom's Taxonomy. *British Journal of Educational Technology*, 51(2), 418-439. <https://doi.org/10.1111/bjet.12831>.
6. Billingsley, B., & Bettini, E. (2019). Supporting students with disabilities in inclusive classrooms: Personnel preparation, collaboration, and instructional strategies. *Intervention in School and Clinic*, 54(5), 295-303. <https://doi.org/10.1177/1053451218823451>.
7. Brown, Q. L., & Greenfield, D. B. (2021). Personalized learning and data-driven education: A close look at the impacts and risks. *Education and Information Technologies*, 26(5), 5171-5188. <https://doi.org/10.1007/s10639-021-10458-x>.
8. Davis, K., & Weinstein, E. (2017). The ethical challenges of ubiquitous learning technologies in K-12 environments. *Theory and Research in Education*, 15(3), 249-265. <https://doi.org/10.1177/1477878517734458>.
9. Feng, W. C., & Liu, Z. (2018). Data privacy in education: An overview of the landscape. *Journal of Educational Computing Research*, 56(5), 645-672. <https://doi.org/10.1177/0735633117727598>
10. Ferguson, R., Macfadyen, L. P., & Clow, D. (2021). Ethical challenges in the use of learning analytics. *Journal of Learning Analytics*, 8(1), 1-15. <https://doi.org/10.18608/jla.2021.7389>.

11. Greenhow, C., & Chapman, A. (2020). Social media and education: Reconceptualizing the boundaries of formal and informal learning. *Learning, Media and Technology*, 45(1), 31-42. <https://doi.org/10.1080/17439884.2019.1704816>.
12. Ifenthaler, D., & Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology Research and Development*, 64, 923-938. <https://doi.org/10.1007/s11423-016-9477-y>
13. Johnson, N. (2017). Customizable modalities for individualized learning. *Journal of e-Learning and Knowledge Society*, 13(2), 9-25.
14. Liu, C. H., & Metcalfe, A. W. (2021). Educational policy and data security: Protecting student privacy in the digital age. *Policy Futures in Education*, 19(1), 112-129. <https://doi.org/10.1177/1478210320922550>.
15. Taylor, L., & Floridi, L. (2020). Group privacy: New challenges of data technologies. *Philosophical Transactions of the Royal Society A*, 378(2163), 20190185. <https://doi.org/10.1098/rsta.2019.0185>.
16. Warner, T., & Mokeyane, K. (2017). Data protection in the cloud: The insider threat to the enterprise. *Information Security Journal: A Global Perspective*, 26(6), 261-274. <https://doi.org/10.1080/19393555.2017.1380055>.
17. Zeide, E. (2017). The structural consequences of big data-driven education. *Big Data & Society*, 4(1). <https://doi.org/10.1177/2053951717717744>.