A Systematic Literature Review of Data Privacy in AI-Driven Educational Platforms

Sibusisiwe Dube[1], Banele Mpande[2], Tiese Chazuza[3], Thembelihle Siwela[4], Musawenkosi Moyo[5], & Sinokubekezela Princess Dube[6]

[1]Lecturer, National University of Science and Technology, Department of Informatics and Analytics, Zimbabwe

[2-3,4,5]Student, National University of Science and Technology, Department of Informatics and Analytics, Zimbabwe

[6]Student. The University of Zambia, School of Engineering, Zambia

DOI: https:/doi.org/10.47772/IJRISS.2026.1026EDU0078

Received: 28 January 2026; Accepted: 02 February 2026; Published: 16 February 2026

ABSTRACT

Artificial Intelligence (AI) driven educational platforms are transforming education towards personalized learning. Despite the affordances of AI-driven education platforms, concerns about data privacy, ethical issues in data handling, and regulatory compliance limit their widespread adoption. Adding to this is the limited literature that comprehensively explains the types of AI-driven educational platforms, their challenges, and the strategies for ensuring data privacy in them. This study presents findings from a Systematic Literature Review (SLR), guided by the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) model. Included in this study were 27 journal articles drawn from Science Direct, IEEE, Springer Nature Link, and Google Scholar. The results of this study categorized the AI-driven educational platforms into Learning Management Systems (LMSs), adaptive learning, intelligent tutoring systems, learning analytics, and AI-personalized learning platforms, AI-enabled educational tools and automated scoring systems, and general AI education systems. Furthermore, several challenges of these AI-driven educational platforms were identified, which include data privacy, data breaches, bias, and the implementation of the AI-driven educational platforms. The strategies for ensuring data privacy include data encryption, user authentication, regular audits, adherence to the General Data Protection Regulation (GDPR), and differential privacy. These results facilitate the development of policies for ensuring that the AI-based educational platforms are secure, considering the large volumes of data that are collected by these and used in systems.

Key Words: Artificial Intelligence, AI-Driven Education Platforms, Data, Privacy, Conceptual Framework

INTRODUCTION

Artificial intelligence (AI) has revolutionized educational platforms and improved teaching and learning experiences for both students and educators (Chen et al., 2020; Pedro et al., 2019). Integrating AI into educational platforms enhances personalized learning, improves student engagement, and provides tutors with useful feedback (Chen et al., 2020). AI-driven educational platforms such as Moodle offer personalized learning platforms, automatic grading, and data-driven insights that significantly improve educational outcomes (Kaleci, 2025; Dube, 2017). These AI-powered systems also improve students' engagement and involvement in learning through smart features such as automation and language translation, and also facilitate easier access to learning environments (Chen et al., 2022; Lin, 2023).

Moodle is an abbreviation for Modular Object-Oriented Dynamic Learning Environment. It is an open-source learning management system (LMS) that is widely adopted by universities, colleges, and other educational

institutions throughout the world (Gamage et al., 2022). Moodle embeds AI capabilities such as adaptive learning algorithms, automated grading, and advanced data analytics (Gamage et al., 2022). It is the most popular and the most preferred learning management system as compared to other educational platforms (Altinpulluk & Kesim, 2021; Dube & Scott, 2018). Moodle dominates in terms of its high rate of acceptance by institutions, and it accommodates a wide range of courses in many different languages (Sergis et al., 2017). Moodle's powerful AI-driven features, like adaptive learning algorithms and data analytics, make the learning experience easy and flawless, but they also necessitate the collection and processing of sensitive student data (Gligorea et al., 2023; Khan et al., 2022). AI makes use of algorithms in a learning management system and depends on data such as student performance metrics, behavioral patterns, and engagement data. (Gligorea et al., 2023; Khosravi et al., 2022).

While AI features improve educational experiences, they raise ethical questions about data security and privacy, especially in regard to the possibility of data breaches (Wang et al., 2023; Nguyen et al., 2023; Golda et al., 2024). These results indicate a gap within the learning management system in that there is a lack of real-time threat detection and response time. These practices need strict privacy measures such as data anonymization, encryption, and differential privacy to mitigate these risks (Razi et al., 2025; Ndlovu et al., 2022). Sensitive information such as student records, personal details, and academic performance must be protected and kept safe to ensure privacy when students, teachers, and others involved are using the learning management system (LMS). To ensure this requires strong data protection measures, secure data storage protocols, and clear communication about data usage policies (Malhotra et al., 2021). This study seeks to explore the data privacy issues associated with AI-driven educational platforms. It seeks to address how security is breached, strategies that are implemented, and the types of AI-driven educational platforms that exist.

Research Questions

1. What types of digital educational platforms exist?
2. How is security breached in AI-driven educational platforms?
3. What security strategies are implemented for AI-driven educational platforms?

METHODOLOGY

This study adopted the PRISMA model to systematically identify relevant studies on data privacy in AI-driven educational platforms (Moodle). The review process was carried out in November 2024, with searches conducted across multiple digital libraries using the query specified in the search

Research Protocol

Specific keywords were used to search the following databases: IEEE, ScienceDirect, SpringerLink, and Google Scholar. The following search string was used to explore the databases: ((“Data privacy” OR “Data security” OR “Data safety” OR “Data safekeeping”) AND (“Artificial Intelligence driven” OR “AI driven”) AND (“Education” OR “Learning” OR “Studying”) AND (“Platforms”)). Depicted in Table 1 is the research protocol showing the database(s), time interval, and inclusion and exclusion criteria.

Table 1.1The research Protocol

Protocol	**Description**
Database(s)	Science Direct, IEEE, Springer Nature Link, and Google Scholar.
Time interval	2020 - 2025
Inclusion criteria	Peer-reviewed journal articles on data privacy in AI-driven education platforms, written in the English Language and published between 2020 and 2025.

Exclusion criteria	Articles published in languages other than English.

The initial search for journal articles resulted in 118 articles, and the final assessment returned 27 articles that met the inclusion criteria, results which are depicted in Figure 1.1. Table 1.1 further extrapolates the key literature relating to the types of AI-driven educational platforms, the challenges faced when using these platforms, and the strategies for ensuring data privacy when applying the AI-driven educational platforms..

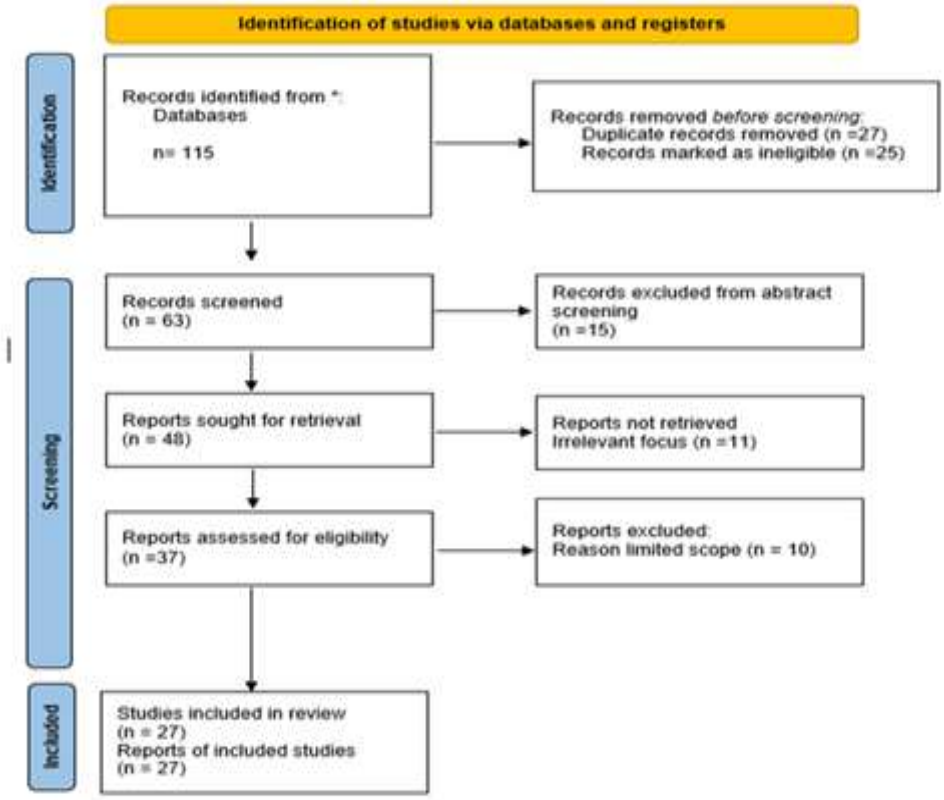

Figure1.1 PRISMA flow diagram for the included articles

Table 1.2 presents the findings from the literature by grouping studies that reported similar educational platforms, security challenges, and mitigation strategies.

Table 1.2 Extracted Data from Included Studies

Sources	**Educational platforms**	**Security challenges of educational platforms**	**Security strategies implemented in AI-driven educational platforms**
(Qazi et al., 2024; Al-Hamad, 2022a; Saqr et al., 2024; Mutimukwe et al., 2022; Alier et al., 2021)	Learning Management System (LMS) • Moodle • Blackboard • Canvas • Talent LMS • Edmodo • Coursera	• Data privacy concerns • Data breaches • Surveillance risks • Lack of transparency • Adoption barriers • User training challenges	• Encryption • Secure authentication • Enhanced privacy controls • GDPR compliance • Transparency measures • Regular security audits

	• edX		
(Patel, 2024; Arslan, 2021; Xu, 2025; Nguyen et al., 2023; Rehan, 2024; Alotaibi, 2024; Oyebola Ayeni et al., 2024)	Adaptive Learning and Intelligent Tutoring System • Adaptive learning systems • Intelligent tutoring systems • AI-driven adaptive platforms	• Privacy infringement • Unauthorized access • Algorithmic bias • Inequality/digital divide • Accountability gaps • Integration complexity	• Data encryption • Student data anonymization • Secure access control • Ethical AI guidelines • Bias mitigation/testing • Compliance with data protection regulations
(Ali et al., 2024; Chima Abimbola Eden et al., 2024; Huang, 2023; Khalil et al., 2025)	Learning Analytics and AI-Personalized Learning Platform • Learning analytics systems • AI-enabled learning systems • Personalized learning platforms	• Centralized data collection risks • Vulnerability to adversarial attacks • Inadequate accountability • Lack of transparency • Privacy breaches	• Federated learning • Resilience testing • Data anonymization • Enhanced accountability measures • Transparency practices • Encryption
(Bognár et al., 2024; Fu et al., 2020; Seprum & Wongwatkit, 2022)	AI-enabled educational tools and automated scoring systems • AI-based chat tools • AI-enabled language e-learning systems • AI automatic scoring applications	• Data privacy risks • Information leakage • Biased algorithms • User data insecurity	• Informed consent • Secure information management • Encryption • Data anonymization • Regular security audits • Ethical AI deployment practices
(Kumar & Choudhury, 2023; Rawamangun Muka et al., 2023; Korobenko et al., 2024; Muli, 2024; Borenstein & Howard, 2021)	General AI education systems • General AI-driven educational systems (non-platform specific)	• Ethical dilemmas • Lack of governance frameworks • Human rights violations • Data misuse • Cybercrime risks • Regulatory compliance challenges	• Ethical frameworks • Governance processes • Privacy-preserving frameworks • Regulatory compliance measures • Rights-based AI principles • Robust authentication and permission management

RESULTS AND DISCUSSION

This section details the results and findings from the included research articles.

Types of Educational Platforms

Our review in Figure 1.2 shows a clear hierarchy in platform adoption. Adaptive AI systems are the leaders, with almost one-third of the reviewed studies referring to them. The systems come with a promise of a bespoke learning experience and can adapt to the weaknesses and strengths of a student automatically, which is an enticing objective of educators who want to stop teaching one-size-fits-all (Arslan, 2021; Patel, 2024). Conventional Learning Management Systems (LMS) like Moodle and Blackboard are at the forefront, and 23% of the literature mentions them. This is not surprising, as it has been proven in literature that these two LMSs are the backbone of the online classroom, and it provides an entire set of tools to manage the course. Because Moodle is an open-source solution, it is a cheaper alternative to many educational institutions (Saqr et al., 2024). Nevertheless, in spite of the popularity of these two LMSs, literature is paying more attention to the ethical and security implications rather than their fundamental functionality (Gamage et al., 2022). Less frequently cited platforms such as Canvas (15%), TalentLMS (8 percent), etc., are likely indicative of the fact that the newer tools are not exclusively used; rather, they are being co-developed with and, in many instances, through the established models of older LMS systems.

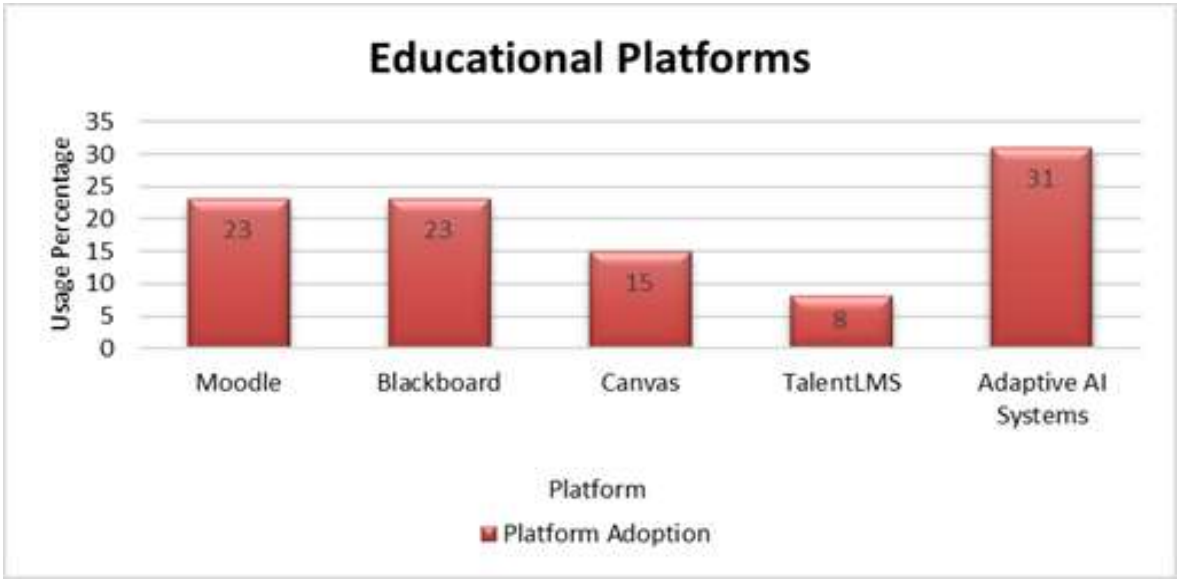

Figure 1.2. Types of Educational Platforms

Challenges with Educational Platforms

The challenges raised in the 27 reviewed articles resulted in the following two problems: data privacy issues (35%) and data breaches (28%), as depicted in Figure 1.3. Such results demonstrate that the researchers and practitioners have a serious concern regarding the safety of the large, sensitive information that is gathered by these platforms. Current sources admit that it is not merely related to test results, but also behavioral data, interaction history, and personal information are harmful sources should they be breached (Gligorea et al., 2023). Moreover, this research found contradictory literature results. Although the risk of algorithmic bias (19%) is always indicated as a significant ethical risk, the discussion of data privacy is not unanimous. Other studies consider bias as an independent fairness concern (Gligorea et al., 2023), but others, such as Huang (2023), note that an insufficiency of transparency in how the data is used can not only allow but also violate data privacy. This is an acute transparency issue since it should be evident how an AI-driven educational platform arrives at the decisions to allow an evaluation of what data the interested AI-driven educational platform is abusing or neglecting (a bias and privacy issue).

The next challenge is the complexity of implementation (18%), which is a significant privacy risk factor since complex systems are difficult to protect. In case of integration issues by institutions, vital security measures such

as anonymizing data appropriately or having frequent audits may be ignored, or they may be executed insufficiently. Al-Hamad (2022) also adds that poor user interaction with the complicated features of the platform can cause security blind spots because users can avoid or misinterpret privacy settings. Finally, the issues that have been raised in this paper are interrelated. For example, not only are hackers causing data privacy to be compromised, but so are opaque algorithms, poorly implemented systems, and disengaged users (Al-Hamad, 2022).

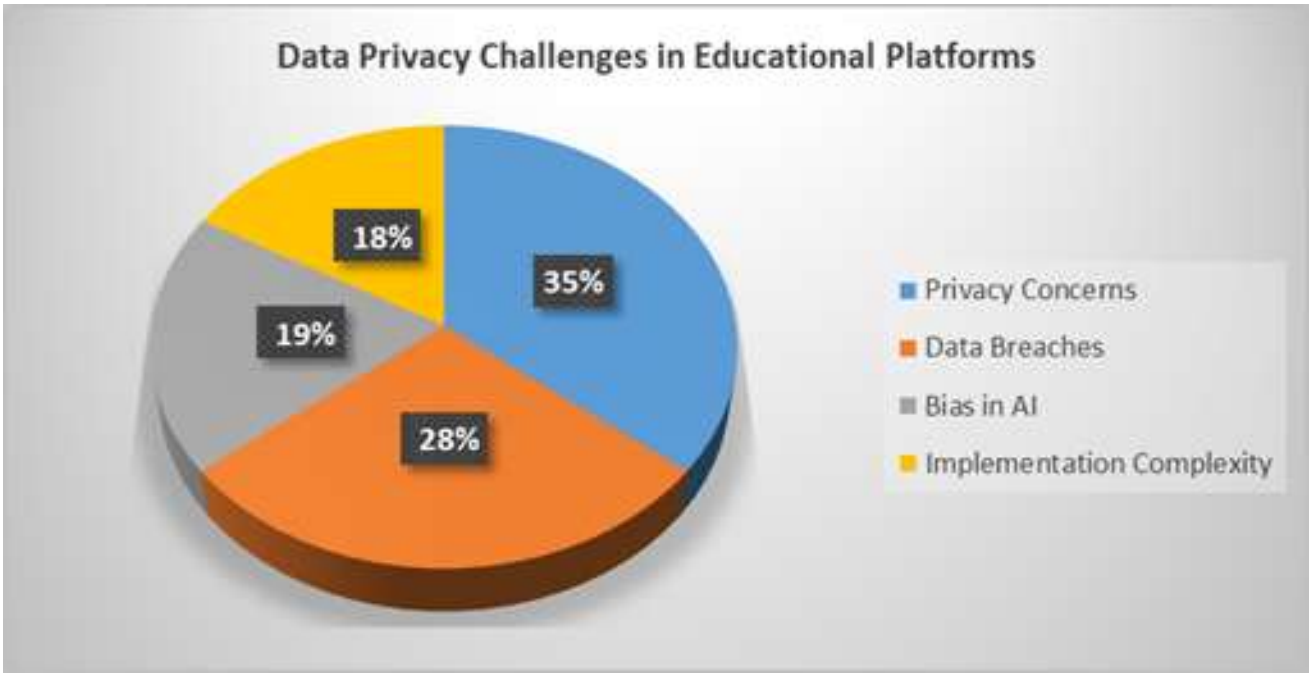

Figure 1.3. Data Privacy Challenges in AI-Driven Platforms

Data Security Strategies in AI-Driven Education Platforms

The identified strategies discussed in the literature that have been taken into consideration in this paper are a combination of both technical and regulatory strategies, as illustrated in Figure 1.4. The most recommended strategies, on the technical side, are encryption (30%) and secure authentication (25%). They are the online counterparts of a good key and a strong lock, necessary but minimal. Qazi et al. (2024) are correct in pairing them with regular security audits (20%), and it can be stated that in rapidly developing AI systems, even security procedures cannot be overlooked or assumed. The regulation component has prevailed upon by the GDPR compliance (15%). Although this is essential to the functioning of law and the development of trust, there was an intriguing lapse in the dialogue. Several articles, including Alotaibi (2024), view GDPR as a process of data processing.

The number of regulators that delve into regulations such as GDPR is small; for instance, data minimization and purpose limitation as active, everyday design concepts of AI in education are rarely considered. A more effective proactive approach to privacy is to design systems that capture the minimum amount of data. The most unadopted approach in the literature review was differential privacy (10%). It is an information processing method that incorporates statistics into datasets to enable analysis without revealing records. This low adoption in these studies is probably due to its technical complexity and the fact that it is still emerging from computer science labs and into mainstream educational technical practice. Nevertheless, its existence foreshadows the future, where learning analytics will have more power. Such techniques as differential privacy will play an essential role in the process of striking a balance between insight and individual anonymity. Overall, these results indicate that the current literature is skewed in favor of instant, technical protection (encryption, authentication) instead of progressive, design-oriented principles (privacy-by-design, data minimization) or sophisticated privacy protection methods (differential privacy). The approaches that have been cited in this paper are more of a checklist as opposed to what is desired: a layered defense, well-built technical controls, steered by well-built ethical principles, and audited on a regular basis within a well-established law framework.

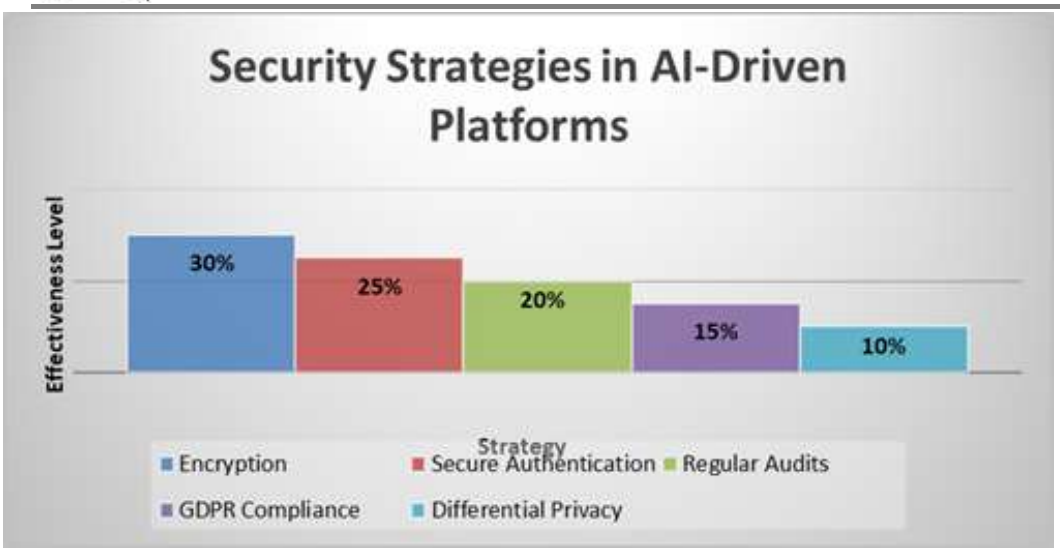

Figure 1.4. Security Strategies in AI-Driven Platforms

Conceptual Framework

The conceptual framework in Figure 1.5 explains how the implementation of AI-driven educational platforms, including learning management systems, adaptive AI systems, and intelligent tutoring systems, creates critical data privacy risks, such as data breaches, algorithmic bias, complexity of implementation, and poor transparency and accountability. Such challenges require the creation and implementation of data privacy mitigation strategies that work on technical and regulatory-ethical tiers. Technical strategies contain measures such as data encryption, secure authentication, anonymization, and differential privacy, whereas regulatory and ethical strategies are concerned with adherence to data protection laws, sound data governance policies, ethical guidelines on AI, and employee training and awareness. All of these mitigation measures will help in achieving improved outcomes in AI-driven educational platforms.

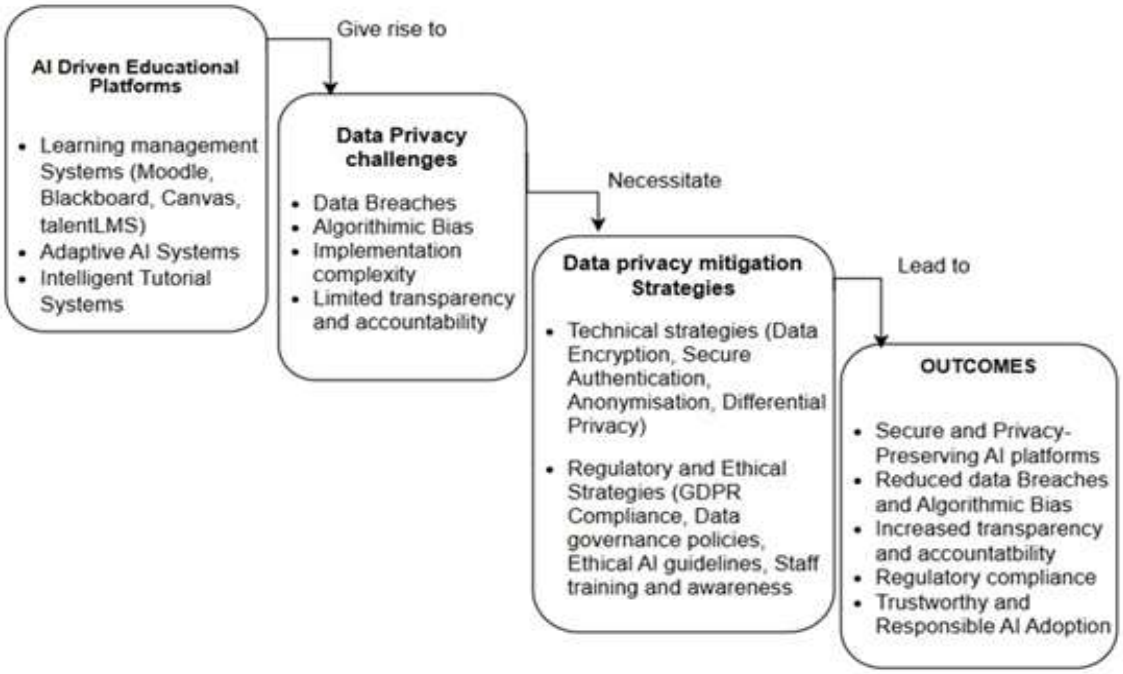

Figure 1.5. Conceptual framework

CONCLUSION

This study aimed to investigate the data privacy challenges in AI-driven learning management platforms. The research utilized a systematic literature review guided by the PRISMA process and identified 27 articles from

an initial pool of 115 records. The findings show that the majority of institutions have embraced Moodle because of its low cost and adaptability. Four data privacy dilemmas have been identified, including privacy concerns, data breaches, algorithmic bias, and implementation complexity. While encryption is the most popular security strategy adopted, differential privacy and compliance with the GDPR have not been properly adopted relative to other security strategies. It also observed a gap that learning management systems offer no means for timely threat detection and remediation of true threats. With better encryption, access control, bias mitigation, and privacy-preserving algorithms, educational institutions should build robust security-based systems to protect user privacy in LMS platforms. For these reasons, training IT staff about AI security must be one of the concerns, and ethical review committees, automated threat detection, and others should be put in place while closely scrutinizing the financial and technical basis of AI-driven platforms to be chosen.

REFERENCES

1. Al-Hamad, N. Q. Moodle As a Learning Management System: Perceived Efficacy and Actual Use. In Journal of Educators Online (Vol. 19, Issue 3), 2022a, https://doi.org/10.9743/JEO.2022.19.3.2
2. Al-Hamad, N. Q. Moodle As a Learning Management System: Perceived Efficacy and Actual Use. Journal of Educators Online, 19(3), 2022b, https://doi.org/10.9743/JEO.2022.19.3.2
3. Ali, M., Siddique, A., Aftab, A., Kamran Abid, M., Fuzail, M., & Abid, K. AI-Powered Customized Learning Paths: Transforming Data Administration for Students on Digital Platforms. Journal of Computing & Biomedical Informatics, 06(02), 2024, https://doi.org/10.56979/602/2024
4. Alier, M., Casañ Guerrero, M. J., Amo, D., Severance, C., & Fonseca, D. Privacy and e-learning: A pending task. Sustainability (Switzerland), 13(16), 2021, https://doi.org/10.3390/su13169206
5. Alotaibi, N. S. The Impact of AI and LMS Integration on the Future of Higher Education: Opportunities, Challenges, and Strategies for Transformation. In Sustainability (Switzerland) (Vol. 16, Issue 23). Multidisciplinary Digital Publishing Institute (MDPI), 2024, https://doi.org/10.3390/su162310357
6. Altinpulluk, H., & Kesim, M. A Systematic Review of the Tendencies in the Use of Learning Management Systems. Turkish Online Journal of Distance Education, 22(3), 1–14, 2021, https://doi.org/10.17718/tojde.961812
7. Arslan, A. An Empirical Design Model for an AI-enabled Learning System. 8(8), 153–167, 2021
8. Bognár, L., Ágoston, G., Bacsa-Bán, A., Fauszt, T., Gubán, G., Joós, A., Juhász, L. Z., Kocsó, E., Kovács, E., Maczó, E., Mihálovicsné Kollár, A. I., & Strauber, G. Re-Evaluating Components of Classical Educational Theories in AI-Enhanced Learning: An Empirical Study on Student Engagement. Education Sciences, 14(9), 974, 974,2024, https://doi.org/10.3390/educsci14090974
9. Borenstein, J., & Howard, A. Emerging challenges in AI and the need for AI ethics education. AI and Ethics, 1(1), 61–65, 2021, https://doi.org/10.1007/s43681-020-00002-7
10. Chen, L., Chen, P., & Lin, Z. Artificial Intelligence in Education: A Review. IEEE Access, 8, 75264–75278, 2020, https://doi.org/10.1109/ACCESS.2020.2988510
11. Chima Abimbola Eden, Olabisi Oluwakemi Adeleye, & Idowu Sulaimon Adeniyi. A review of AI-driven pedagogical strategies for equitable access to science education. Magna Scientia Advanced Research and Reviews, 10(2), 044–054, 2024, https://doi.org/10.30574/msarr.2024.10.2.0043
12. Dube, S., and Scott, E. The organizational constraints of blending e-learning tools in education: Lecturers' perceptions, Information Technology-New Generations: 14th International Conference on Information Technology. Springer International Publishing, 2018.
13. Dube, S. Educators' pedagogical concerns on blending ICTs in teaching. In European Conference on e-Learning (pp. 150-155). Academic Conferences International Limited, 2017
14. Fu, S., Gu, H., & Yang, B. The affordances of AI-enabled automatic scoring applications on learners' continuous learning intention: An empirical study in China. British Journal of Educational Technology, 51(5), 1674–1692, 2020, https://doi.org/10.1111/bjet.12995
15. Gamage, S. H. P. W., Ayres, J. R., & Behrend, M. B. A systematic review on trends in using Moodle for teaching and learning. International Journal of STEM Education, 9(1), 2022, https://doi.org/10.1186/s40594-021-00323-x
16. Gligorea, I., Cioca, M., Oancea, R., Gorski, A. T., Gorski, H., & Tudorache, P. Adaptive Learning Using Artificial Intelligence in e-Learning: A Literature Review. Education Sciences, 13(12), 2023, https://doi.org/10.3390/educsci13121216

17. Golda, A., Mekonen, K., Pandey, A., Singh, A., Hassija, V., Chamola, V., & Sikdar, B. Privacy and Security Concerns in Generative AI: A Comprehensive Survey. IEEE Access, 12(April), 48126–48144, 2024, https://doi.org/10.1109/ACCESS.2024.3381611
18. Huang, L. Ethics of Artificial Intelligence in Education: Student Privacy and Data Protection. Science Insights Education Frontiers, 16(2), 2577–2587, 2023, https://doi.org/10.15354/sief.23.re202
19. Kaleci, D. Integration and application of artificial intelligence tools in the Moodle platform: A theoretical exploration, 2025
20. Khalil, M., Shakya, R., & Liu, Q. Towards Privacy-Preserving Data-Driven Education: The Potential of Federated Learning, 2025, https://doi.org/10.1109/ICTCS65341.2025.10989403
21. Khan, M. A., Khojah, M., & Vivek. Artificial Intelligence and Big Data: The Advent of New Pedagogy in the Adaptive E-Learning System in the Higher Educational Institutions of Saudi Arabia. Education Research International, 2022, 1–10, 2022. https://doi.org/10.1155/2022/1263555
22. Khosravi, H., Shum, S. B., Chen, G., Conati, C., Tsai, Y. S., Kay, J., Knight, S., Martinez-Maldonado, R., Sadiq, S., & Gašević, D. Explainable Artificial Intelligence in Education. Computers and Education: Artificial Intelligence, 3(March), 2022, https://doi.org/10.1016/j.caeai.2022.100074
23. Korobenko, D., Nikiforova, A., & Sharma, R. Towards a Privacy and Security-Aware Framework for Ethical AI: Guiding the Development and Assessment of AI Systems. ACM International Conference Proceeding Series, 740–753, 2024, https://doi.org/10.1145/3657054.3657141
24. Kumar, S., & Choudhury, S. Normative ethics, human rights, and artificial intelligence. AI and Ethics, 3(2), 441–450, 2023, https://doi.org/10.1007/s43681-022-00170-8
25. Lin, J. ChatGPT and Moodle Walk into a Bar: A Demonstration of AI's Mind-blowing Impact on E-Learning. SSRN Electronic Journal, 2018, 2023, https://doi.org/10.2139/ssrn.4393445
26. Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C. Internet of Things: Evolution, concerns, and security challenges. Sensors, 21(5), 1–35, 2021, https://doi.org/10.3390/s21051809
27. Muli, M. Legal and Ethical Implications of Data Privacy in Artificial Intelligence: A Review of Data Privacy Among Learners in Kenyan Secondary Schools. Journal of the Kenya National Commission for UNESCO, 5(1), 2024, https://doi.org/10.62049/jkncu.v5i1.170
28. Mutimukwe, C., Viberg, O., Oberg, L. M., & Cerratto-Pargman, T. Students' privacy concerns in learning analytics: Model development. British Journal of Educational Technology, 53(4), 932–951, 2022, https://doi.org/10.1111/bjet.13234
29. Ndlovu, B., Dube, S., Dube, S. P., and Mpofu, S. A framework for transitioning to virtual classes during life-threatening pandemics like COVID-19, 21st European Conference on e-Learning ECEL 2022. 2022.
30. Nguyen, A., Ngo, H. N., Hong, Y., Dang, B., & Nguyen, B. P. T. Ethical principles for artificial intelligence in education. Education and Information Technologies, 28(4), 4221–4241, 2023, https://doi.org/10.1007/s10639-022-11316-w
31. Oyebola Olusola Ayeni, Nancy Mohd Al Hamad, Onyebuchi Nneamaka Chisom, Blessing Osawaru, & Ololade Elizabeth Adewusi. AI in education: A review of personalized learning and educational technology. GSC Advanced Research and Reviews, 18(2), 261–271, 2024, https://doi.org/10.30574/gscarr.2024.18.2.0062
32. Patel, S. AI-driven educational interventions: an empirical study on their efficacy. 9(2), 145–156, 2024
33. Pedro, F., Subosa, M., Rivas, A., & Valverde, P. Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development. Education Sector: United Nations Educational, Scientific, and Cultural Organization. Ministerio de Educación, 1–46, 2019, https://en.unesco.org/themes/education-policy-
34. Qazi, S., Kadri, M. B., Naveed, M., Khawaja, B. A., Khan, S. Z., Alam, M. M., & Su'ud, M. M. AI-Driven Learning Management Systems: Modern Developments, Challenges, and Future Trends during the Age of ChatGPT. Computers, Materials and Continua, 80(2), 3289–3314, 2024, https://doi.org/10.32604/cmc.2024.048893
35. Rawamangun Muka, J., Gadung, P., Jakarta Timur, K., & Khusus, D. Ethical Problems of Digitalization and Artificial Intelligence in Education: A Global Perspective. Journal of Pharmaceutical Negative Results, 14(2), 2150–2161, 2023, https://doi.org/10.47750/pnr.2023.14.S02.254

36. Razi, Q., Piyush, R., Chakrabarti, A., & Singh, A. Enhancing Data Privacy: A Comprehensive Survey of Privacy-Enabling Technologies. IEEE Access, 13(January), 40354–40385, 2025, https://doi.org/10.1109/ACCESS.2025.3546618
37. Rehan, H. Shaping the Future of Education with Cloud and AI Technologies: Enhancing Personalized Learning and Securing Data Integrity in the Evolving EdTech Landscape Shaping the Future of Education with Cloud and AI Technologies: Enhancing Personalized Learning. April 2023, 2024
38. Revesai, Z. Ethical Implications of AI-Driven Education Systems on Digital Rights: A Comparative Analysis. June 2024
39. Neehalika Bavya, S.P.Blessina Bashapaka & Suvarchala Reddy, G. An Empirical Study on the Role of Artificial Intelligence in Human Capital Management. International Research Journal on Advanced Engineering and Management (IRJAEM), 2(03), 223–227, 2024, https://doi.org/10.47392/irjaem.2024.0035
40. Saqr, R. R., Al-Somali, S. A., & Sarhan, M. Y. Exploring the Acceptance and User Satisfaction of AI-Driven e-Learning Platforms (Blackboard, Moodle, Edmodo, Coursera, and edX): An Integrated Technology Model. Sustainability (Switzerland), 16(1), 2024, https://doi.org/10.3390/su16010204
41. Seprum, P., & Wongwatkit, C. Trends and issues of immersive learning environments in higher education from 2001 to 2020: Perspectives on adaptive ubiquitous learning experiences. International Journal of Mobile Learning and Organization, 16(1), 95–122, 2022, https://doi.org/10.1504/IJMLO.2022.119966
42. Sergis, S., Vlachopoulos, P., Sampson, D. G., & Pelliccione, L. Handbook on Digital Learning for K-12 Schools. Handbook on Digital Learning for K-12 Schools, October 2017, https://doi.org/10.1007/978-3-319-33808-8
43. Wang, M., Qin, Y., Liu, J., & Li, W. Identifying personal physiological data risks to the Internet of Everything: the case of facial data breach risks. Humanities and Social Sciences Communications, 10(1), 1–15, 2023, https://doi.org/10.1057/s41599-023-01673-3
44. Wu, Y. Revolutionizing Learning and Teaching: Crafting Personalized, Culturally Responsive Curriculum in the AI Era. Creative Education, 15(08), 1642–1651, 2024, https://doi.org/10.4236/ce.2024.158098
45. Xu, X. W. AI optimization algorithms enhance higher education management and personalized teaching through empirical analysis. Scientific Reports, 15(1), 1–18, 2025, https://doi.org/10.1038/s41598-025-94481-5