19 - 21 December 2025 Berlin , Germany

Safeguarding The Future: AI-Driven Data Governance and Cybersecurity in K-12 Education

Nidhi Srivastava

Oakland University, The United States

Abstract

A sudden digitalization of the K-12 education has placed data governance as one of the urgent priorities of the school, and sensitive student, teacher, and institutional data should be handled with responsibility. The paper addresses the modern data governance situation in K-12 schools and identifies such obstacles as the adherence to privacy regulations, data insecurity, and ethical use of learning analytics. It is based on recent academic works and evaluates case studies and best practices that can help K-12 institutions to institute solid governance frameworks, by engaging stakeholders, integrating policies, and leveraging new technologies. This study analyzes AI-driven models predicting cybersecurity losses in K-12 education. Results show Random Forest outperforms Linear Regression with lower RMSE and higher accuracy. Feature importance analysis reveals 2022 losses as the strongest predictor, followed by earlier years. Findings highlight longitudinal data's value and ensemble methods' superiority for forecasting risks and guiding policy. Future directions are also taken into account in the paper, which requires the resilience of governance models to deal with cybersecurity threats and integration of artificial intelligence and fair access to digital resources. This paper identifies the significance of secure, transparent and adaptive governance mechanisms in guaranteeing trust and accountability in managing educational data by synthesising the evidence presented in the latest scholarship.Artificial intelligence-based solutions may offer significant efficacy and personalized learning, encompassing administrative analysis and adaptive learning; however, they are also associated with a vast array of cybersecurity threats that most educational institutions are currently ill-equipped to address (King, 2025). K-12 organizations are the main targets of ransomware, phishing, and data breaches because they have a lot of sensitive student information, old infrastructure, limited funds, and not enough technical knowledge (King, 2025). AI has made school cyber security better, in fact. For instance, AI-based software that finds unusual behaviour can help people follow COPPA and FERPA privacy rules better and lower the risk of data breaches (Obioha Val, 2024). However, new vices, cryptic algorithms, unequal accessibility, and possible algorithmic bias have all been brought about by the use of AI. Strong data governance

frameworks must be established for these reasons (Umoke et al., 2025). The community's and parents' attitudes are also concerning because, according to a recent PDK survey, nearly seven out of ten parents oppose sharing student data with AI systems. This indicates a high degree of mistrust and privacy concerns (Education, 2025). It is evident from this conflict between stakeholder interests and technological advancement how challenging it is to establish AI-controlled governance and advanced cybersecurity in schools. In this paper, the target of the research is to discuss the way AI can be utilized to enhance data governance and cybersecurity in the K-12 education sector and map a way that will not put technological innovation in the spotlight but instead provide ethical integrity and resilience in the digital era.
?

Keywords: Data Governance; K-12 Education; Student Data Privacy; Cybersecurity; Educational Technology; Learning Analytics; Best Practices; Resilience