Chapter 8
Safeguarding Student Data:
Privacy and Security Challenges in AI-Powered Education Tools

Md Mehedi Hasan Emon
https://orcid.org/0000-0002-6224-9552
American International University-Bangladesh, Bangladesh

Most. Sharmin Ara Chowdhury
https://orcid.org/0009-0005-1050-8283
National University Bangladesh, Bangladesh

ABSTRACT

This chapter explores the critical privacy and security challenges posed by AI-powered education tools. It examines how AI enhances student support and personalized learning while highlighting risks associated with chatbots, data collection, and processing. Ethical concerns, including consent and fairness, are discussed alongside the complexities of global regulations such as GDPR and FERPA. The chapter also addresses cybersecurity threats targeting educational AI systems and presents strategies to mitigate these risks. Emerging privacy-preserving techniques like federated learning and differential privacy are evaluated for their potential to safeguard student data. Drawing on case studies, it identifies best practices for ethical AI

DOI: 10.4018/979-8-3373-3316-8.ch008

implementation and offers actionable recommendations for educators and policymakers. Finally, this chapter underscores the need for a balanced approach that protects student privacy without stifling innovation in AI-driven education.

INTRODUCTION

Artificial intelligence (AI) is now being used more often in educational institutions and is changing how they teach, test and connect with students. The use of these technologies such as adaptive platforms and AI assistants brings great improvements in tailored help and time saved for students. At the same time, there are major worries about how student information is being handled regarding privacy, safety and governance. This chapter focuses on how to protect the personal information of students using AI at schools and why it is important. At the beginning of the chapter, the role of AI in helping students learn and supporting teachers is introduced, explaining how AI tools assist in communication, offer personal advice and encourage students to take part actively. Although these applications support education in many ways, they use a lot of data which leads to questions about its handling and security. Privacy Risks in AI-Powered Chatbots and Virtual Assistants is the section that looks at the risks that may arise when educators rely on AI chatbots and virtual assistants. Because these systems instantaneously record student data, there is a risk that this data might be used or watched by people who should not access it if the systems are not safeguarded properly. Moving forward, Data Collection, Storage and Processing in AI Education Tools discusses what happens to student data and how it is handled and points out how this could be a concern when third parties or cloud services are involved. The section discusses how institutions can be held accountable and points out the dangers caused by either amassing too much data or not being tightly regulated. The chapter afterward addresses moral issues in AI-Driven Learning Systems such as what constitutes informed consent, how algorithms can show biases, the importance of student autonomy and the threat of inequalities being reinforced by hidden computer-based decisions. Although these ethical issues were usually ignored while developing AI, they are now