Federated Learning in Education: Enhancing Student Privacy in AI-Based Feedback Mechanisms

Suman Vij, Suneetha K.S

Shree Guru Gobind Singh Tricentenary University (SGT University), St. Claret Autonomous College

Federated Learning in Education: Enhancing Student Privacy in AI-Based Feedback Mechanisms

[1]Suman Vij, Professor, Faculty of Commerce & Management, Shree Guru Gobind Singh Tricentenary University (SGT University), Gurugram, Haryana, India. sumanvij2000@gmail.com

[2]Suneetha K.S, Assistant Professor, Department of Commerce, St. Claret Autonomous College, Bangalore, Karnataka, India suneetha@claretcollege.edu.in

Abstract

Federated Learning (FL) offers a groundbreaking approach to developing AI models in educational settings by preserving data privacy while enabling personalized learning experiences. By keeping sensitive student data local to their devices, FL mitigates the risks associated with traditional centralized systems, ensuring compliance with stringent privacy regulations such as the GDPR and the FERPA. This book chapter explores the integration of Federated Learning into educational contexts, with a particular focus on adaptive learning systems, privacy-enhancing mechanisms, and the ethical and legal considerations crucial for successful implementation. The role of model aggregation, balancing performance with privacy concerns, was critically analyzed, alongside the impact of Federated Learning on personalized education, student data security, and system scalability. Key challenges in data heterogeneity and ensuring fairness in AI models are also discussed, highlighting strategies for overcoming these obstacles. By addressing both the technical and regulatory aspects, this chapter provides a comprehensive overview of the potential of Federated Learning to revolutionize education while ensuring that privacy, equity, and legal compliance remain paramount.

Keywords: Federated Learning, Data Privacy, Adaptive Learning Systems, GDPR, FERPA, Model Aggregation.

Introduction

FL was emerging as a powerful paradigm for machine learning, particularly in privacy-sensitive environments such as education [1]. Traditional machine learning models require centralized collection and storage of vast amounts of data, creating potential risks regarding data security and privacy breaches [2]. Federated Learning addresses these challenges by enabling machine learning models to be trained across multiple decentralized devices without the need for raw data to be exchanged [3]. Instead of transferring personal or sensitive data to central servers, local devices share only aggregated model updates, thus preserving data privacy [4]. This shift has vast implications for the education sector, where student data must be handled with the utmost care. The decentralized nature of FL makes it an ideal candidate for enhancing data privacy while still leveraging machine learning to improve educational experiences through personalized learning solutions [5].

Educational institutions increasingly turn to AI-based technologies to support adaptive learning systems, the integration of Federated Learning can significantly enhance the ability to provide personalized education while safeguarding students' sensitive information [6-8]. Adaptive learning systems use data-driven insights to tailor educational content to individual students, helping them progress at their own pace. FL can optimize these systems by ensuring that each student's data remains on their personal device, contributing to a model that adapts to their learning preferences and challenges [9]. This ability to tailor educational experiences without compromising privacy represents a significant advancement in the way educational institutions use AI. FL supports scalable, efficient, and secure implementation, which was crucial for large-scale deployments in schools, universities, and online educational platforms [10].

The application of Federated Learning in education introduces unique challenges. One of the most significant hurdles was ensuring that models trained on data from diverse sources remain fair and effective [11]. Educational data was highly heterogeneous, with students coming from varying socio-economic, geographical, and cultural backgrounds. Federated Learning models must therefore account for this diversity to avoid bias in the final global model [12]. The decentralized nature of FL requires the development of sophisticated model aggregation techniques that can combine local updates from multiple devices while maintaining performance and accuracy [13-16]. These challenges necessitate the development of advanced algorithms and protocols to ensure that Federated Learning systems are robust, equitable, and can deliver the desired outcomes for all students [17].

The technical challenges, there are also substantial ethical and legal considerations that must be addressed when implementing Federated Learning in education [18]. Regulatory frameworks such as the GDPR in Europe and the FERPA in the United States impose strict requirements on the handling of student data [19]. Federated Learning's privacy-preserving design aligns well with these regulations, but it was crucial for educational institutions to ensure full compliance [20]. This involves transparent data governance practices, obtaining explicit consent from students or their guardians, and ensuring that data was anonymized and protected at all stages of model training. Institutions must have clear procedures in place to address any potential data breaches or misuse, which could have significant legal and reputational consequences [21].

These challenges, the potential benefits of Federated Learning in education are substantial. FL can enable the development of adaptive learning systems that are not only personalized and efficient but also privacy-conscious and legally compliant [22]. By addressing both the technological and regulatory challenges, Federated Learning can serve as a key enabler for the next generation of educational tools [23]. As educational institutions continue to embrace AI and machine learning, Federated Learning offers a pathway that balances innovation with responsibility [24,25]. This chapter explore the role of Federated Learning in education, focusing on its impact on adaptive learning systems, its challenges, and the ethical and legal frameworks that guide its implementation, providing a comprehensive view of its potential to revolutionize education.