MODERN CRYPTOGRAPHIC FRAMEWORKS FOR EDUCATIONAL DATA PROTECTION

Oleg Kyrychenko, Oleksandr Shmatko
National Technical University «Kharkiv Polytechnic Institute», Kharkiv

The digital transformation of education has led to the exponential growth of sensitive student data, intensifying the need for robust privacy-preserving mechanisms. This study examines modern approaches to educational data security, focusing on tokenization, encryption, differential privacy, federated learning, and secure multi-party computation (MPC). Tokenization is emphasized as a practical method for replacing sensitive student identifiers with non-sensitive placeholders, thereby enabling data protection without compromising usability. Vault-based and vaultless tokenization models offer different trade-offs between performance and scalability, especially when integrated into real-time learning management systems.

Complementary techniques such as encryption and differential privacy enhance data confidentiality during storage, transmission, and analysis. While traditional encryption like AES-256 is foundational, homomorphic encryption offers a breakthrough by allowing computation on encrypted data, though it remains computationally intensive. Differential privacy, by contrast, introduces statistical noise to data outputs, enabling institutions to publish aggregate information without revealing individual identities–an approach adopted by government initiatives like the U.S. Department of Education's College Scorecard [1].

Federated learning further decentralizes model training by keeping raw data on local devices, sharing only model updates with central servers. This technique is especially relevant in multi-institutional contexts, supporting collaborative improvement of educational tools while preserving data sovereignty [2]. Blockchain also emerges as a key enabler for secure credential verification, with bibliometric analyses highlighting its growing application in academic certification and institutional governance [3].

While each of these technologies offers unique advantages, their combined implementation is essential to establishing a comprehensive privacy framework. This study advocates for a modular, interoperable tokenization system that integrates seamlessly with existing educational infrastructures, addressing regulatory compliance while enabling data-driven innovation. Future research should prioritize optimizing advanced cryptographic methods for real-time deployment and expanding privacy-aware AI applications in smart learning environments.

References:

1. Priedigkeit M., Weich A., Schiering I. Privacy and Identity Management. Springer, 2020.
2. Jiang H., Yu R., Liu J. //*IEEE Trans. on Industrial Informatics*. 2021. Vol. 17(4), P. 2484–2493.
3. Jain R., Seth N., Sood K., Grima S. Digital Transformation. Springer, 2023. P. 53–66.