Privacy-Preserving Techniques in Federated Learning

Grace Moyo

2024-01-29

Core Techniques

- Differential privacy
- Secure aggregation
- Decentralized training

Implications

- Data protection in edge computing
- Real-world deployment barriers