World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:19, No:01, 2025

Convergence and Stability in Federated Learning with Adaptive Differential Privacy Preservation

Authors : Rizwan Rizwan

Abstract : This paper provides an overview of Federated Learning (FL) and its application in enhancing data security, privacy, and efficiency. FL utilizes three distinct architectures to ensure privacy is never compromised. It involves training individual edge devices and aggregating their models on a server without sharing raw data. This approach not only provides secure models without data sharing but also offers a highly efficient privacy--preserving solution with improved security and data access. Also we discusses various frameworks used in FL and its integration with machine learning, deep learning, and data mining. In order to address the challenges of multi--party collaborative modeling scenarios, a brief review FL scheme combined with an adaptive gradient descent strategy and differential privacy mechanism. The adaptive learning rate algorithm adjusts the gradient descent process to avoid issues such as model overfitting and fluctuations, thereby enhancing modeling efficiency and performance in multi-party computation scenarios. Additionally, to cater to ultra-large-scale distributed secure computing, the research introduces a differential privacy mechanism that defends against various background knowledge attacks.

Keywords : federated learning, differential privacy, gradient descent strategy, convergence, stability, threats
Conference Title : ICCSCIT 2025 : International Conference on Computer Science, Cybersecurity and Information Technology
Conference Location : Sydney, Australia
Conference Dates : January 28-29, 2025