National Conference on Latest Innovations in Engineering, Science, Management and Humanities (NCLIESMH – 2024)

26th May, 2024, Raipur, Chhattisgarh, India.

CERTIFICATE NO : NCLIESMH /2024/C0524593

A Study of Federated Learning for Privacy-Preserving Data Analysis

Vishal Trivedi

Research Scholar, Department of Comp Science and Engineering,
P.K. University, Shivpuri, M.P., India.

ABSTRACT

Federated learning for privacy-preserving data analysis focuses on a modern machine learning approach that enables multiple users or organizations to collaboratively train models without sharing their raw data. In traditional data analysis methods, data is collected and stored in a central server, which raises concerns about privacy, security, and data misuse. Federated learning addresses these issues by allowing data to remain on local devices while only model updates, such as parameters or gradients, are shared with a central system. This decentralized approach reduces the risk of data breaches and ensures better compliance with privacy regulations. It is especially useful in sensitive fields like healthcare, finance, and mobile applications, where user data must be protected. The study also examines the efficiency, accuracy, and challenges of federated learning, including communication costs, system heterogeneity, and potential security threats like model poisoning. Despite these challenges, federated learning provides a promising solution for secure and privacy-aware data analysis. It helps organizations gain valuable insights from distributed data while maintaining user trust and confidentiality.