IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

A Comprehensive Review of Federated Learning Techniques for Privacy-Preserving Cybersecurity Applications

Bipin Balu Shinde
Lecturer, Department of Computer Technology
Amrutvahini Polytechnic, Sangamner

Abstract: *In an era marked by the exponential growth of cyber threats and data privacy concerns, Federated Learning (FL) has emerged as a transformative paradigm in machine learning that emphasizes privacy-preserving, decentralized model training. Unlike traditional centralized approaches, FL enables multiple clients—such as edge devices or organizational nodes—to collaboratively train a shared model while keeping raw data localized. This review explores FL applications in cybersecurity, including intrusion detection, malware classification, biometric authentication, and IoT security. It further discusses privacy-enhancing techniques like differential privacy, homomorphic encryption, and secure aggregation. Despite its promise, FL faces challenges such as non-IID data, communication overhead, and adversarial threats. The paper outlines mitigation strategies and future research directions, offering a comprehensive foundation for understanding FL's role in secure, collaborative threat intelligence.*

Keywords: Federated Learning, Cybersecurity, Privacy-Preserving Machine Learning, Intrusion Detection, Edge Computing, Secure Aggregation, Non-IID Data, Blockchain, Explainable AI

DOI: 10.48175/IJARSCT-28153