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 4, April 2025

Impact Factor: 7.67

Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection

Niravkumar Prajapati
Independent Researcher
niravprajapati343@gmail.com

Abstract: *Federated Learning's (FL) distributed threat detection technique is a significant advancement in cybersecurity as it preserves privacy while processing data in a decentralized manner. Centralized security systems that rely on raw data collection present two major threats to users because they create regulatory problems in addition to data breaches. FL removes security concerns through its model-building process, allowing different organizations to work together without sharing private data. This document investigates FL's role in cybersecurity through an analysis of malware/ransomware detection, IDS applications, secure threat detection, and network traffic anomaly detection. The paper explores effective privacy-protecting techniques: FL implementations are protected against Byzantine and backdoor attacks using Secure Multi-Party Computation (SMPC), Homomorphic Encryption (HE), Differential Privacy (DP), and Secure Model Aggregation. FL delivers advantages but encounters challenges mainly related to excessive communication demands as well as performance deterioration under adversarial conditions, and difficulties with system expansion. The research provides an exhaustive analysis of FL-based cybersecurity frameworks while discussing existing applications and security threats together with future developments for these systems and the need for advanced privacy-protecting methods to improve the dependability of FL cybersecurity solutions.*

Keywords: Federated Learning, Privacy-Preserving Cybersecurity, Secure Threat Detection, Intrusion Detection Systems, Differential Privacy, Secure Multi-Party Computation, Anomaly Detection

DOI: 10.48175/IJARSCT-25168