Federated Learning Trade-offs in IoT Security: Communication Overhead vs. Adversarial Robustness

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 13 peer-reviewed papers addressing the following research question: What is the trade-off between communication overhead and model robustness against adversarial attacks in federated learning systems for IoT security. Federated learning (FL) is revolutionizing healthcare by enabling collaborative machine learning across institutions while preserving patient privacy and meeting regulatory standards. This review delves into FL's applications within smart health systems, particularly its. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.0/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Federated Learning in Smart Healthcare: A Comprehensive Review on Privacy, Security, and Predictive Analytics with IoT Integration. Research question: What is the trade-off between communication overhead and model robustness against adversarial attacks in federated learning systems for IoT security?.

2 Methodology

Systematic literature search across multiple databases yielded 13 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.0/10.

3 Results

13 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 3.0/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

References

- https://doi.org/10.1109/sp.2019.00065
- https://doi.org/10.1109/jsac.2021.3126076
- https://doi.org/10.3390/healthcare12242587