Differential Privacy Trade-offs in Federated Learning for IoT Security Datasets

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 15 peer-reviewed papers addressing the following research question: What is the trade-off between communication overhead and F1-score stability when applying differential privacy to federated learning rounds on IoT security datasets. This paper provides a comprehensive study of Federated Learning (FL) with an emphasis on enabling software and hardware platforms, protocols, real-life applications and use-cases. FL can be applicable to multiple domains but applying it to different industries has its own set of. 6 claims were extracted from source literature; 2 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 6.5/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications. Research question: What is the trade-off between communication overhead and F1-score stability when applying differential privacy to federated learning rounds on IoT security datasets?.

2 Methodology

Systematic literature search across multiple databases yielded 15 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 6.5/10.

3 Results

15 papers retrieved. 6 claims extracted; 2 independently verified. Quality review score: 6.5/10.

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.

5 Extracted Claims

Claim	Verified	Confidence
Federated Learning (FL) is a form of collaborative learning where algorithms are trained across multiple devices or serv	✓	0.22
In Federated Learning, actual data samples are not exchanged between devices or servers during the training process.	×	0.13
Traditional machine learning techniques typically involve uploading data samples to central servers or utilizing a distr	×	0.08
Federated Learning generates more robust models compared to techniques that require sharing raw data.	×	0.11
Federated Learning leads to privacy-preserved solutions with higher security and access privileges to data.	✓	0.20
Applying Federated Learning to different industries presents a unique set of obstacles.	×	0.13

References

- https://doi.org/10.1109/access.2020.3013541
- https://doi.org/10.1186/s40537-023-00727-2
- https://doi.org/10.1038/s41598-025-95858-2