Differential Privacy Trade-offs in Federated Code Generation Model Fine-Tuning

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 3 peer-reviewed papers addressing the following research question: What is the trade-off between inference latency and model robustness against adversarial attacks when applying differential privacy mechanisms to federated fine-tuning of code generation models. Federated learning (FL) is a machine learning setting where many clients (e.g., mobile devices or whole organizations) collaboratively train a model under the orchestration of a central server (e.g., service provider), while keeping the training data decentralized. FL embodies. 10 claims were extracted from source literature; 10 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 8.2/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Advances and Open Problems in Federated Learning. Research question: What is the trade-off between inference latency and model robustness against adversarial attacks when applying differential privacy mechanisms to federated fine-tuning of code generation models?.

2 Methodology

Systematic literature search across multiple databases yielded 3 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 8.2/10.

3 Results

3 papers retrieved. 10 claims extracted; 10 independently verified. Quality review score: 8.2/10.

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 machine learning setting where many clients collaboratively train a model under the orchest	✓	0.43
In federated learning, clients include entities such as mobile devices or whole organizations.	✓	0.16
In federated learning, the central server is typically a service provider.	✓	0.17
Federated learning keeps the training data decentralized.	✓	0.18
Federated learning embodies the principles of focused data collection and minimization.	✓	0.32
Federated learning can mitigate systemic privacy risks resulting from traditional, centralized machine learning and data	✓	0.40
Federated learning can mitigate costs resulting from traditional, centralized machine learning and data science approach	✓	0.35
There has been an explosive growth in federated learning research.	✓	0.16
The monograph discusses recent advances in federated learning.	✓	0.26
The monograph presents an extensive collection of open problems and challenges in federated learning.	✓	0.35

References

- https://doi.org/10.1561/2200000083
- https://doi.org/10.1109/access.2021.3140175
- https://doi.org/10.1109/jproc.2021.3054390