Robustness of Federated Code Generation Models Under Dynamic Client Availability

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 13 peer-reviewed papers addressing the following research question: What is the impact of varying client availability schedules on the robustness of federated code generation models against backdoor injections. The delicate equilibrium between user privacy and the ability to unleash the potential of distributed data is an important concern. Federated learning, which enables the training of collaborative models without sharing of data, has emerged as a privacy-centric solution. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.2/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Adversarial Robustness Unhardening via Backdoor Attacks in Federated Learning. Research question: What is the impact of varying client availability schedules on the robustness of federated code generation models against backdoor injections?.

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 3.2/10.

3 Results

13 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 3.2/10.

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.

References

- http://arxiv.org/abs/2305.01267v1
- http://arxiv.org/abs/2310.11594v3
- http://arxiv.org/abs/2306.08011v1