Byzantine Attack Mitigation in Federated Malware Detection Under Heterogeneous Client Participation

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 9 peer-reviewed papers addressing the following research question: What is the impact of varying client participation rates and data heterogeneity on the effectiveness of Byzantine attack mitigation strategies in federated learning-based malware detection frameworks. To deal with the increasing number of cyber-attacks, intrusion detection system (IDS) plays an important role in monitoring and ensuring the security of the computer network. With the power of machine learning and deep learning, intelligent IDS systems have gained increasing. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 1.5/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Personalized federated learning-based intrusion detection system: Poisoning attack and defense. Research question: What is the impact of varying client participation rates and data heterogeneity on the effectiveness of Byzantine attack mitigation strategies in federated learning-based malware detection frameworks?.

2 Methodology

Systematic literature search across multiple databases yielded 9 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 1.5/10.

3 Results

9 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 1.5/10.

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.

References

- https://doi.org/10.1016/j.future.2023.10.005
- https://doi.org/10.1109/access.2021.3075203
- https://doi.org/10.1109/access.2021.3118642