Soft Label Strategies and Robustness in Adversarially Trained Tabular Foundation Models

Assignee Research

June 9, 2026

Abstract

This report synthesises findings from 11 peer-reviewed papers addressing the following research question: What is the impact of different soft label generation strategies (e.g., confidence-based, temperature scaling) on the robustness of adversarially trained tabular foundation models against label. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.7/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Implicit Generative Modeling of Random Noise during Training for Adversarial Robustness. Research question: What is the impact of different soft label generation strategies (e.g., confidence-based, temperature scaling) on the robustness of adversarially trained tabular foundation models against label noise, evaluated using F1-score degradation on TabM-NAR with 20% random label corruption?.

2 Methodology

Systematic literature search across multiple databases yielded 11 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.7/10.

3 Results

11 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 3.7/10.

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/1807.02188v4
- http://arxiv.org/abs/2512.03307v1
- http://arxiv.org/abs/2405.04191v1