Code Property Graph Fidelity and GCN-Based False Positive Prediction Accuracy in SAST Tools

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 5 peer-reviewed papers addressing the following research question: What is the correlation between Code Property Graph representation fidelity and the classification accuracy of GCN-based false positive predictors across diverse SAST tools. Software vulnerabilities pose significant security challenges and potential risks to society, necessitating extensive efforts in automated vulnerability detection. There are two popular lines of work to address automated vulnerability detection. 5 claims were extracted from source literature; 5 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 8.7/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Comparison of Static Application Security Testing Tools and Large Language Models for Repo-level Vulnerability Detection. Research question: What is the correlation between Code Property Graph representation fidelity and the classification accuracy of GCN-based false positive predictors across diverse SAST tools?.

2 Methodology

Systematic literature search across multiple databases yielded 5 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 8.7/10.

3 Results

5 papers retrieved. 5 claims extracted; 5 independently verified. Quality review score: 8.7/10.

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.

5 Extracted Claims

Claim	Verified	Confidence
SAST tools obtain low vulnerability detection rates with relatively low false positives.	✓	0.33
LLMs can detect up to 90% to 100% of vulnerabilities but suffer from high false positives.	✓	0.26
By further ensembling the SAST tools and LLMs, the drawbacks of both SAST tools and LLMs can be mitigated to some extent	✓	0.29
The study compared 15 diverse SAST tools with 12 popular or state-of-the-art open-source LLMs.	✓	0.30
The study focused on detecting software vulnerabilities from repositories of three popular programming languages: Java,	✓	0.22

References

- https://doi.org/10.48550/arxiv.2407.16235
- https://doi.org/10.3390/electronics15050918
- https://doi.org/10.1007/s10664-021-10029-x