Adversarial Code Obfuscation Impact on Llama3 and DeepSeek R1 Vulnerability Detection

Assignee Research

June 4, 2026

Abstract

This report synthesises findings from 9 peer-reviewed papers addressing the following research question: How does adversarial code obfuscation affect the vulnerability detection F1-score of Llama3 versus Deepseek R1 on the Big-Vul dataset. 9 claims were extracted from source literature; 9 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.9/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Deep Learning Approach for Intelligent Intrusion Detection System. Research question: How does adversarial code obfuscation affect the vulnerability detection F1-score of Llama3 versus Deepseek R1 on the Big-Vul dataset?.

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 7.9/10.

3 Results

9 papers retrieved. 9 claims extracted; 9 independently verified. Quality review score: 7.9/10.

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
Machine learning techniques are widely used to develop intrusion detection systems (IDS) for detecting and classifying c	✓	0.29
Malicious attacks are continually changing and occurring in very large volumes.	✓	0.22
Different malware datasets are available publicly for research by the cyber security community.	✓	0.30
No existing study has shown a detailed analysis of the performance of various machine learning algorithms on various pub	✓	0.35
Publicly available malware datasets need to be updated systematically and benchmarked due to the dynamic nature of malwa	✓	0.24
The paper explores a deep neural network (DNN) to develop an IDS for detecting and classifying unforeseen and unpredicta	✓	0.24
Various datasets used for evaluation were generated over the years through static and dynamic approaches.	✓	0.20
The paper presents a comprehensive evaluation of experiments comparing DNNs and other classical machine learning classif	✓	0.18
The evaluation was conducted on various publicly available benchmark malware datasets.	✓	0.23

References

- https://doi.org/10.1109/access.2019.2963724
- https://doi.org/10.1109/access.2019.2895334
- https://doi.org/10.14722/ndss.2018.23198