Mul-GAD Semi-Supervised Anomaly Detection Outperforms Unsupervised GNN Models on Cross-Domain Datasets

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 9 peer-reviewed papers addressing the following research question: To what extent does Mul-GAD's semi-supervised approach improve anomaly detection accuracy over fully unsupervised GNN models like OCSVM-GNN on cross-domain datasets such as Amazon and DBLP, using. Machine learning techniques are being widely used to develop an intrusion detection system (IDS) for detecting and classifying cyberattacks at the network-level and the host-level in a timely and automatic manner. However, many challenges arise since malicious attacks are. 10 claims were extracted from source literature; 10 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 6.9/10. 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: To what extent does Mul-GAD's semi-supervised approach improve anomaly detection accuracy over fully unsupervised GNN models like OCSVM-GNN on cross-domain datasets such as Amazon and DBLP, using evaluation metrics like AUC-ROC and F1-score?.

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 6.9/10.

3 Results

9 papers retrieved. 10 claims extracted; 10 independently verified. Quality review score: 6.9/10.

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	✓	0.31
Malicious attacks are continually changing and occurring in very large volumes.	✓	0.23
Different malware datasets are publicly available for cybersecurity research.	✓	0.16
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	✓	0.23
A Deep Neural Network (DNN) is a type of deep learning model.	✓	0.25
The paper explores a DNN to develop an IDS capable of detecting and classifying unforeseen and unpredictable cyberattack	✓	0.16
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 classical machine learning classifiers.	✓	0.18
The evaluation was conducted on various publicly available benchmark malware datasets.	✓	0.23

References

- https://doi.org/10.1038/s41524-022-00734-6
- https://doi.org/10.1109/access.2019.2947484
- https://doi.org/10.1109/access.2019.2895334