

IGRF-RFE Hybrid Feature Selection for LLM-Based Log Anomaly Detection

Assignee Research

June 9, 2026

Abstract

This report synthesises findings from 10 peer-reviewed papers addressing the following research question: Can the IGRF-RFE hybrid feature selection strategy be effectively transferred to enhance LLM-based log analysis for anomaly detection, and how does its performance compare on sequence-based security. 9 claims were extracted from source literature; 2 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 4.5/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: IGRF-RFE: A Hybrid Feature Selection Method for MLP-based Network Intrusion Detection on UNSW-NB15 Dataset. Research question: Can the IGRF-RFE hybrid feature selection strategy be effectively transferred to enhance LLM-based log analysis for anomaly detection, and how does its performance compare on sequence-based security benchmarks?.

2 Methodology

Systematic literature search across multiple databases yielded 10 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 4.5/10.

3 Results

10 papers retrieved. 9 claims extracted; 2 independently verified. Quality review score: 4.5/10.

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.

5 Extracted Claims

Claim	Verified	Confidence
The experiments were conducted on a desktop running Ubuntu 20.04.4 LTS with 16GB RAM, AMD Ryzen 7 2700 processor, and an	×	0.01
The experimental environment was based on Python 3.8 and TensorFlow 2.4.1.	×	0.03
The UNSW-NB15 dataset contains 2.5 million records of data, covering one normal class and nine attack classes.	×	0.08
The UNSW-NB15 dataset consists of 49 features divided into six groups: flow features, basic features, content features,	×	0.08
The UNSW-NB15 dataset contains 39 numerical features and 3 categorical features.	×	0.10
Data preprocessing techniques included data cleaning, minority removal, oversampling, encoding, and normalization.	×	0.03
The dataset was divided into a training set, a validation set, and a test set.	×	0.02
The proposed method involves ensemble feature selection based on information gain and random forest importance, followed	✓	0.25
Information gain (IG) is a univariate filter feature selection method based on information entropy.	✓	0.21

References

- <http://arxiv.org/abs/2604.12218v1>
- <http://arxiv.org/abs/2203.16365v2>
- <http://arxiv.org/abs/2406.16308v1>