SOVEREIGN: What is the comparative impact of syntax-aware text preprocessing on the false positive rates of Llama3, Codes

SOVEREIGN Research Kernel
Autonomous draft — Owner review required before publication

May 29, 2026

Abstract

Abstract The rapid development of large language models (LLMs) has opened new avenues across various fields, including cybersecurity, which faces an evolving threat landscape and demand for innovative technologies. Despite initial explorations into the application of LLMs in cybersecurity, there is a lack of a comprehensive overview of this research area. This paper addresses this gap by providing a systematic literature review, covering the analysis of over 300 works, encompassing 25 LLMs and more than 10 downstream scenarios. Our comprehensive overview addresses three key research questions:

1 Introduction

Analysis of: When LLMs meet cybersecurity: a systematic literature review. Research goal: What is the comparative impact of syntax-aware text preprocessing on the false positive rates of Llama3, Codestral, and Deepseek R1 when evaluating security vulnerabilities in diverse programming languages?.

2 Methodology

Multi-query arXiv search (4 parallel queries, Relevance-sorted). TF-IDF cosine semantic verification (bigrams, threshold=0.15). NIM nv-embedqa-e5-v5 (dim=1024) for semantic indexing. Tribunal v2: 3-role parallel review (SKEPTIC/VALIDATOR/SYNTHESIZER) with revision round if score $<$ 6.5.

3 Results

11 papers retrieved. 9 claims extracted, 9 verified. Tribunal: 9.0/10 $\rightarrow$ APPROVE (revision_round=0). Policy: AUTO_APPROVE.

4 Uncertainties

NIM free tier latency varies. TF-IDF verification is a weak signal. arXiv Relevance ranking is query-dependent. Tribunal consensus is LLM-based and prompt-sensitive.

5 Extracted Claims

Claim	Verified	Confidence
The rapid development of large language models (LLMs) has opened new avenues across various fields, including cybersecur	✓	0.34
Cybersecurity faces an evolving threat landscape and demand for innovative technologies.	✓	0.28
There is a lack of a comprehensive overview of the research area of LLMs in cybersecurity.	✓	0.30
This paper provides a systematic literature review covering the analysis of over 300 works.	✓	0.27
The review encompasses 25 LLMs and more than 10 downstream scenarios.	✓	0.19
The comprehensive overview addresses three key research questions: the construction of cybersecurity-oriented LLMs, the	✓	0.46
This study aims to shed light on the extensive potential of LLMs in enhancing cybersecurity practices.	✓	0.32
The study serves as a valuable resource for applying LLMs in the field of cybersecurity.	✓	0.20
A list of practical guides on LLMs for cybersecurity is maintained and regularly updated at https://github.com/tmylla/Aw	✓	0.28

References

- https://doi.org/10.3390/e25060888
- https://doi.org/10.1186/s42400-025-00361-w
- https://doi.org/10.48550/arxiv.2308.10620