Sequence Length Effects on Efficiency-Accuracy Trade-offs in Retrieval-Augmented Llama Models for Long-Context Code Vulnerability Detection

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 11 peer-reviewed papers addressing the following research question: What is the impact of input sequence length on the efficiency-accuracy trade-off in retrieval-augmented Llama3-70B compared to Llama-13B for long-context code tasks like vulnerability detection. The escalating complexity of cyber threats, coupled with the rapid evolution of digital landscapes, poses significant challenges to traditional cybersecurity mechanisms. This review explores the transformative role of LLMs in addressing critical challenges in cybersecurity. 7 claims were extracted from source literature; 5 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.0/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: From Vulnerability to Defense: The Role of Large Language Models in Enhancing Cybersecurity. Research question: What is the impact of input sequence length on the efficiency-accuracy trade-off in retrieval-augmented Llama3-70B compared to Llama-13B for long-context code tasks like vulnerability detection?.

2 Methodology

Systematic literature search across multiple databases yielded 11 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 7.0/10.

3 Results

11 papers retrieved. 7 claims extracted; 5 independently verified. Quality review score: 7.0/10.

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
Traditional security mechanisms often fall short in detecting, mitigating, and responding to complex risks due to the es	✓	0.40
LLMs such as GPT, BERT, and PaLM demonstrate capabilities in natural language processing that enable them to parse vast	✓	0.22
LLMs are capable of identifying vulnerabilities and automating threat detection.	×	0.07
Applications of LLMs in cybersecurity extend to phishing detection, malware analysis, drafting security policies, and in	✓	0.30
LLMs enhance organizational resilience against cyberattacks by leveraging features like context awareness and real-time	✓	0.26
LLMs facilitate more informed decision-making in cybersecurity contexts.	×	0.11
Deploying LLMs in cybersecurity presents challenges including issues of interpretability, scalability, ethical concerns,	✓	0.28

References

- https://doi.org/10.3390/computation13020030
- https://doi.org/10.48550/arxiv.2406.00515
- https://doi.org/10.3390/electronics13071361