Chapter 5
Performance Evaluation of LLM-Based Security Systems

Yara Shamoo
Saint Leo University, USA

ABSTRACT

This chapter delves into the performance evaluation of large language model (LLM)-based security systems, focusing on their effectiveness, scalability, and adaptability in dynamic threat landscapes. By examining various performance metrics, including accuracy, speed, and resource utilization, the chapter provides a comprehensive analysis of how these systems compare to traditional security approaches. Furthermore, it explores the challenges of evaluating LLMs in real-world scenarios and discusses potential improvements to enhance their robustness. This evaluation aims to guide future developments in LLM-based security systems, ensuring they meet the rigorous demands of modern cybersecurity.

INTRODUCTION

The rapid advancement of Artificial Intelligence (AI) and, more specifically, Large Language Models (LLMs) has significantly impacted various domains, including cybersecurity. These models, known for their ability to process and understand vast amounts of natural language data, have shown promising results in enhancing security systems. This chapter aims to provide a detailed performance evaluation of LLM-based security systems, focusing on their strengths, limitations, and the practical implications of their deployment in real-world scenarios.

DOI: 10.4018/979-8-3693-9311-6.ch005

The Rise of LLMs in Cybersecurity

LLMs have emerged as powerful tools in cybersecurity, offering innovative solutions to complex challenges. For instance, the development of domain-specific language models such as SecureBERT demonstrates the potential of tailored LLMs in enhancing security measures (Aghaei et al., 2022). SecureBERT, designed specifically for cybersecurity, exemplifies how LLMs can be fine-tuned to detect and mitigate security threats effectively. Similarly, the exploration of LLMs in detecting Distributed Denial of Service (DDoS) attacks highlights their applicability in safeguarding cyber-physical systems (Guastalla et al., 2023).

The adaptability and efficiency of LLMs in cybersecurity are further underscored by studies that examine their integration with existing security frameworks. Alawida et al. (2023) provide a comprehensive review of ChatGPT, exploring its advancements and limitations in natural language processing (NLP) and cybersecurity. The study highlights how LLMs, like ChatGPT, are being leveraged to address security concerns, though they also present new ethical challenges.

Evaluating LLM-Based Security Systems

Evaluating the performance of LLM-based security systems is a complex task that requires a multi-faceted approach. The effectiveness of these systems is often measured by their accuracy in identifying and mitigating threats, their speed in processing and responding to security incidents, and their scalability in handling large datasets. Ameri et al. (2021) explore these aspects through the fine-tuning of BERT for cybersecurity claim classification, demonstrating the potential of LLMs in enhancing the precision and reliability of security systems.

Another critical factor in evaluating LLM-based security systems is their ability to adapt to evolving threats. The dynamic nature of cyber threats necessitates continuous learning and adaptation, which LLMs are inherently capable of, given their design. Studies like those by Ferrag et al. (2023) and Al-Hawawreh et al. (2023) discuss the role of LLMs in revolutionizing threat detection and the challenges that come with their implementation. These challenges include the computational resources required to train and deploy LLMs, as well as the potential for adversarial attacks that can exploit vulnerabilities in these models.

Practical Applications and Future Directions

The practical applications of LLMs in cybersecurity are vast and varied. From automating threat detection to enhancing the security of communication networks, LLMs have shown potential across multiple facets of cybersecurity. Gao (2023)