Chapter 9
Comparative Analysis of LLMs vs. Traditional Methods in Vulnerability Detection

Yara Shamoo
Saint Leo University, USA

ABSTRACT

In the evolving landscape of cybersecurity, the detection of software vulnerabilities is paramount for ensuring system integrity and protection. This chapter provides a comparative analysis of large language models (LLMs) versus traditional methods in vulnerability detection. It explores the strengths and limitations of each approach, focusing on accuracy, efficiency, adaptability, and scalability. By examining real-world case studies and experimental results, the chapter highlights the transformative potential of LLMs in detecting complex vulnerabilities. It also discusses the implications of integrating LLMs into existing security frameworks and the challenges posed by their adoption. This analysis serves as a guide for practitioners and researchers seeking to optimize vulnerability detection methods in an increasingly dynamic threat environment.

INTRODUCTION

In the modern digital era, the landscape of cybersecurity is constantly evolving, driven by the increasing complexity and frequency of cyber threats. Traditional methods of vulnerability detection, while foundational, are being challenged by the emergence of more sophisticated approaches, notably those powered by artificial

DOI: 10.4018/979-8-3693-9311-6.ch009

intelligence (AI) and machine learning (ML). Among these, Large Language Models (LLMs) have gained significant attention for their potential to revolutionize the way vulnerabilities are detected and mitigated in software systems.

Traditional methods for vulnerability detection have relied heavily on rule-based systems, signature analysis, and heuristic approaches. These methods are effective to a certain extent but often fall short in the face of novel or zero-day vulnerabilities. As cyber threats evolve, the limitations of traditional methods become more pronounced, particularly in their inability to adapt quickly to new attack vectors and their reliance on predefined rules that may not cover all potential threats (Wright, Dawson Jr, & Omar, 2012; Omar, 2022).

In contrast, LLMs, which are a subset of AI techniques, have demonstrated remarkable capabilities in natural language processing (NLP) tasks, including text generation, translation, and sentiment analysis. Their application in cybersecurity, particularly in vulnerability detection, is relatively new but promising. LLMs can analyze large volumes of unstructured data, identify patterns, and generate insights that traditional methods might miss. They offer a dynamic and adaptive approach to threat detection, capable of learning from vast datasets and improving over time (Chaudhary, 2023; Motlagh et al., 2024).

The deployment of LLMs in cybersecurity is not without challenges. Issues such as data privacy, ethical considerations, and the need for robust training datasets are critical factors that must be addressed to harness the full potential of these models (Alawida et al., 2023; Jiang, 2024). Moreover, the integration of LLMs into existing security frameworks poses significant technical and operational challenges, requiring careful consideration of the models' strengths and limitations (Ameri et al., 2021; Sultana et al., 2023).

This chapter aims to provide a comprehensive comparative analysis of LLMs versus traditional methods in vulnerability detection. It will explore the theoretical foundations of each approach, analyze their practical applications, and discuss the potential for integrating LLMs into contemporary cybersecurity strategies. By examining case studies and experimental results, this chapter will highlight the advantages and disadvantages of each method, offering insights into their respective roles in the future of cybersecurity (Ferrag et al., 2023; Gao, 2023).

The rise of LLMs represents a significant shift in the cybersecurity landscape. Their ability to process and analyze complex datasets, coupled with their adaptability and scalability, makes them a powerful tool in the fight against cyber threats. However, their implementation requires a nuanced understanding of both the technological and ethical implications. This chapter will delve into these aspects, providing a balanced perspective on the comparative effectiveness of LLMs and traditional methods in vulnerability detection (Pearce et al., 2023; Gennari et al., 2024).