Chapter 3
Techniques and Approaches for Leveraging LLMs in Security Analysis

Rebet Keith Jones
https://orcid.org/0009-0008-0487-1301
Capitol Technology University, USA

ABSTRACT

This chapter explores the various techniques and approaches for utilizing large language models (LLMs) in security analysis. It delves into how LLMs can enhance the detection and mitigation of security vulnerabilities by leveraging natural language processing and machine learning capabilities. The chapter highlights the integration of LLMs into security frameworks, offering insights into their application in threat detection, anomaly analysis, and automated incident response. Additionally, it examines the challenges and future directions in leveraging LLMs for robust security analysis, emphasizing the need for ongoing research to address current limitations.

INTRODUCTION

The advent of Large Language Models (LLMs) has significantly transformed various fields, including cybersecurity. These models, powered by advanced machine learning algorithms, offer novel approaches to enhancing security measures, particularly in detecting and mitigating cyber threats. LLMs such as GPT-3 and BERT have shown remarkable proficiency in understanding and generating

DOI: 10.4018/979-8-3693-9311-6.ch003

human-like text, which can be leveraged to improve the accuracy and efficiency of cybersecurity systems.

LLMs have been increasingly applied to domain-specific tasks in cybersecurity, such as vulnerability detection, threat analysis, and incident response. For instance, SecureBERT, a domain-specific language model, has been developed to enhance cybersecurity applications by tailoring the BERT architecture to the needs of the security domain (Aghaei et al., 2022). Similarly, Ameri et al. (2021) demonstrated the effectiveness of fine-tuning the BERT model for classifying cybersecurity claims, emphasizing the potential of LLMs in this field.

The application of LLMs in cybersecurity is not without challenges. Issues such as data integration, model scalability, and the ethical implications of deploying these models in real-world scenarios have been extensively discussed in the literature (Alawida et al., 2023; Aldoseri et al., 2023). Moreover, the use of LLMs in automated systems raises concerns about the potential for adversarial attacks and the need for robust defensive mechanisms (Al-Hawawreh et al., 2023; Ferrag et al., 2023).

Recent studies have also explored the use of LLMs for specific cybersecurity tasks, such as detecting Distributed Denial of Service (DDoS) attacks (Guastalla et al., 2023) and performing penetration testing (Happe & Cito, 2023). These applications demonstrate the versatility and growing importance of LLMs in the cybersecurity landscape.

As LLMs continue to evolve, their role in cybersecurity is expected to expand, offering new tools and techniques to address emerging threats. However, the integration of these models into existing security frameworks requires careful consideration of the associated risks and challenges (Gao, 2023; Gennari et al., 2024). This chapter aims to provide a comprehensive overview of the techniques and approaches for leveraging LLMs in security analysis, focusing on their applications, benefits, and potential pitfalls.

TECHNIQUES AND APPROACHES FOR LEVERAGING LLMS IN SECURITY ANALYSIS

Large Language Models (LLMs) have shown immense potential in cybersecurity, offering a range of applications from threat detection to vulnerability assessment. As these models continue to evolve, their role in enhancing cybersecurity measures becomes increasingly prominent.