Chapter 8
Integration of LLMs With Traditional Security Tools

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

Angel Justo Jones
University of Virginia, USA

ABSTRACT

The integration of large language models (LLMs) with traditional security tools represents a significant advancement in the cybersecurity domain. This chapter explores the potential of combining LLMs with established security mechanisms to enhance threat detection, response, and overall system resilience. By analyzing the complementary strengths of LLMs and traditional tools, this chapter highlights how LLMs can augment existing security frameworks, improve anomaly detection, automate security workflows, and address evolving cyber threats. The discussion also includes challenges such as computational complexity, ethical considerations, and integration complexities, offering insights into future research directions.

INTRODUCTION

The rapid evolution of cybersecurity threats has necessitated the integration of advanced technologies to bolster defense mechanisms. Traditional security tools, while effective in many scenarios, are increasingly being supplemented by emerging technologies, including Artificial Intelligence (AI) and Machine Learning (ML). Among these, Large Language Models (LLMs) have shown considerable promise in enhancing cybersecurity operations by offering advanced capabilities in natural

DOI: 10.4018/979-8-3693-9311-6.ch008

language understanding and processing. This chapter explores the integration of LLMs with traditional security tools, examining how this fusion can provide a more robust, adaptive, and intelligent security infrastructure.

LLMs have gained significant attention for their ability to process and generate human-like text, making them valuable in various domains, including cybersecurity. These models, such as GPT-3 and BERT, have been trained on vast amounts of data, enabling them to understand and generate text in a contextually relevant manner. In the context of cybersecurity, LLMs are being leveraged for tasks such as threat detection, incident response, vulnerability analysis, and the automation of routine security tasks.

For instance, SecureBERT, a domain-specific LLM designed for cybersecurity, demonstrates how fine-tuning a language model on cybersecurity-related data can enhance its effectiveness in tasks like identifying security vulnerabilities and classifying cyber threats (Aghaei, Niu, Shadid, & Al-Shaer, 2022). Similarly, CyberBERT, another specialized LLM, has been utilized for cybersecurity claim classification, highlighting the role of LLMs in automating complex cybersecurity tasks (Ranade, Piplai, Joshi, & Finin, 2021).

The integration of LLMs with traditional security tools offers several advantages. First, LLMs can enhance the accuracy and speed of threat detection by analyzing large volumes of textual data, such as logs, alerts, and incident reports, in real time. This capability is particularly useful in identifying patterns that might be missed by conventional tools, thus providing an additional layer of defense (Ferrag et al., 2023).

Moreover, LLMs can assist in automating repetitive tasks, such as generating incident reports or correlating data from different sources, thereby freeing up human analysts to focus on more strategic tasks (Sultana, Taylor, Li, & Majumdar, 2023). The ability of LLMs to understand and process natural language also enables them to interact with human users more effectively, making complex cybersecurity operations more accessible to non-experts (Al-Hawawreh, Aljuhani, & Jararweh, 2023).

Furthermore, LLMs can be integrated into existing security frameworks to provide a more holistic approach to cybersecurity. For example, ChatGPT and other similar models can be used to enhance the capabilities of Security Information and Event Management (SIEM) systems by providing context-aware analyses and recommendations (Alawida, Mejri, Mehmood, Chikhaoui, & Isaac Abiodun, 2023).

Despite the potential benefits, integrating LLMs with traditional security tools also presents several challenges. One of the primary concerns is the computational complexity associated with deploying LLMs in real-time environments. These models require significant processing power and memory, which can strain existing IT infrastructure and lead to increased operational costs (Gao, 2023).