Intrusion Detection through Log Analysis with Large Language Models (LLMs)

Abstract

Intrusion Detection Systems (IDS) generate extensive logs and alerts, making it challenging to identify genuine threats efficiently. This research focuses on applying Large Language Models (LLMs) to analyze system and network logs automatically for suspicious activities. By training or fine-tuning transformer-based LLMs on log datasets, this project aims to classify log entries as malicious or benign or to identify anomalous entries indicative of cyber intrusions. The resulting tool provides practical and accessible intrusion detection capabilities ideal for undergraduate or master's students.

Introduction

The continuous production of system logs—from servers, operating systems, and applications—often contains subtle indicators of cyber threats, such as repeated failed logins, unusual command executions, or abnormal activity sequences. Manual analysis of these logs is impractical due to volume and complexity. Thus, automating this analysis using advanced machine learning techniques such as Large Language Models (LLMs) provides a valuable approach.

This project's goals include:

- Preparing log datasets representing normal operation and attack scenarios.

- Fine-tuning pre-trained LLMs (e.g., DistilBERT or BERT) for log classification or anomaly detection.

- Creating a practical prototype capable of reading and classifying logs to identify potential intrusions.

This practical implementation offers hands-on experience in leveraging NLP models for cybersecurity, demonstrating how artificial intelligence can significantly enhance log-based threat detection.

Related Work

Machine learning applications in log analysis have shown significant promise for detecting anomalies indicative of cyber-attacks. For instance, Du et al. (2017) proposed DeepLog, a deep learning model to detect anomalies from system logs effectively, significantly reducing false-positive rates compared to traditional rule-based methods. Additionally, research by Meng et al. (2019) introduced LogAnomaly, a deep learning-based framework for structured log anomaly detection, demonstrating high accuracy in identifying anomalous log sequences.

Transformer-based models have also emerged as effective tools in analyzing log data. For example, LogBERT (Guo et al., 2021) leveraged transformer architectures for anomaly detection in system logs, significantly improving accuracy and efficiency. Sharma et al. (2021) applied transformer-based models to detect anomalies in Windows event logs, showcasing the model's effectiveness in cybersecurity threat detection scenarios.

These studies collectively demonstrate the feasibility and effectiveness of applying LLMs to log-based intrusion detection, providing a robust foundation for this project's practical implementation.

References

- Du, M., Li, F., Zheng, G., & Srikumar, V. (2017). DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), 1285-1298.

- Meng, W., Liu, Y., Zhu, Y., Zhang, S., Pei, D., Liu, Y., ... & Zhang, R. (2019). LogAnomaly: Unsupervised Detection of Sequential and Quantitative Anomalies in Unstructured Logs. International Joint Conference on Artificial Intelligence (IJCAI), 4739-4745.

- Guo, H., Yuan, S., Wu, X., & Li, Y. (2021). LogBERT: Log Anomaly Detection via BERT. IEEE International Conference on Data Mining (ICDM), 2021.

- Sharma, S., Datta, P., & Malik, H. (2021). Detecting Cyber-Attacks Using Transformer Networks on System Logs. IEEE International Conference on Machine Learning and Applications (ICMLA), 2021.