World Academy of Science, Engineering and Technology
International Journal of Cognitive and Language Sciences
Vol:18, No:11, 2024

Dynamic Log Parsing and Intelligent Anomaly Detection Method Combining Retrieval Augmented Generation (RAG) and Prompt Engineering

Authors : Linxin Liu

Abstract : As system complexity increases, log parsing and anomaly detection become more and more important in ensuring system stability. However, traditional methods often face the problems of insufficient adaptability and decreasing accuracy when dealing with rapidly changing log contents and unknown domains. To this end, this paper proposes a distinct approach, LogRAG, which combines RAG (Retrieval Augmented Generation) technology with Prompt Engineering for Large Language Models, applied to log analysis tasks to achieve dynamic parsing of logs and intelligent anomaly detection. By combining real-time information retrieval and prompt optimization, this study significantly improves the adaptive capability of log analysis and the interpretability of results. Experimental results show that the method performs well on several public datasets, especially in the absence of training data, and significantly outperforms traditional methods. This paper provides a different technical path for log parsing and anomaly detection, demonstrating significant theoretical value and application potential.

Keywords : log parsing, anomaly detection, RAG (Retrieval-Augmented Generation), prompt engineering, LLMs
Conference Title : ICSLP 2024 : International Conference on Speech and Language Processing
Conference Location : San Francisco, United States
Conference Dates : November 04-05, 2024