LLM-Based Anomaly Detection in System Logs

Lam Nguyen
University of Central Florida
la815794@ucf.edu

January 2026

Abstract

A proposal will be given on how Large Language Models can be used to identify problems in system and network logs. The project that will be used is a web application. The framework that will be used is LangChain and Claude in order to perform this task. The topic number in this syllabus is: 14. LLM-Based Anomaly Detection in System Logs: Apply LLMs to identify abnormal patterns in system or network logs

1 Problem Statement

A properly built software application will produce a large amount of Logs that record the ongoing operations of that said application. Overtime a very large amount of logs will be produced and it can be very tedious and time-consuming for a human to go through all these logs, analyze them and spot any abnormal operations.

This is especially true for massive web applications that can have billions of users. LLMs can be used to do this kind of work to spot any anomalies.

2 Proposed Technique

The technique for working with Logging involves 4 steps with the intent of balancing cost-efficiency with utilizing the full power of the LLM. It is not practical to feed millions or billions of lines of logs to an LLM as an LLM uses too much computing power and electricity. Also, it costs money even when accessing an LLM through an API.

The first step is to Parse the Logs. We first group similar logs into templates.

The second step is to perform Vector Search and Contextual Retrieval.This step is intended to provide a baseline of what normal operations and logs from the web application will look like. Retrieval-Augmented Generation will be used to feed the LLM.

The third step is the actual LLM Reasoning that acts as a judge. A suspicious log will be sent to the LLM for it to make a judgment.

The fourth step is to analyze the root cause of all the errors from the series of log entries and explain in human language why the error(s) are occurring.

3 Expected Outcomes

Given the powerful LLM tools that are available such as Claude Sonnet 4.5, it seems likely that that an LLM should be able to analyze logs. This is dependent on the amount of log data produced and the quality of the log data produced.

Too many logs produced that are not processed correctly, or if the wrong type of log data is produced, then this will affect the LLM's ability to spot patterns. So my expectation is that alot of the LLM's ability to spot problems is dependent on the quality of the application's logging system.