Christine Tsai
DS 4002 CS3 - Hook Document
Apr. 11, 2025

Your Task: Use server metric logs to detect anomalies potentially indicative of a Distributed Denial of Service (DDoS) attack

The Scenario:
You work for a tech startup as a systems administrator and you are tasked with finding the most efficient way to detect anomalies that might be indicative of DDoS attacks. Your manager avoids using external tools, so they have asked you to test our own models which may be integrated into the development of internal software in the future. The company is still recovering from a previous DDoS not too long ago, and it is your mission to help the company be more prepared when the next attack strikes.

To help your company avoid losing valuable resources and customers down the line, you will have to rely on data from AWS Cloudwatch server metrics that your company gave you access to. In this study, you will need to clean (if necessary) and analyze the data to detect anomalies within the data using time series modeling techniques. In other words, you're tasked with the following: performing exploratory data analysis, building and training models, and delivering your decision on which model you think is best.

The Deliverable:
You will be producing a report that discusses the results of your analysis and why you selected the model that you did. You will also include visualizations in your report to build your case on why the company can count on this model the next timee your company is the target of a DDoS attack.

Access your materials here:
GitHub Repository Link: https://github.com/rtg7bs/CS3