COMP4651 Chat Bot

Ferdy 20642622
Ng Chak Sang 20767903
Nguyen Kha Nhat Long 20730596

Abstract

This project presents the implementation of a serverless chatbot for image moderation, using OpenFaaS and Kubernetes on an EC2 instance. The chatbot employs multiple serverless functions to handle various tasks, such as image moderation, toxic comments moderation, and chat and image generation functionalities.

Introduction

The increasing popularity of chatbots has led to their widespread use in various domains, such as customer support, marketing, and entertainment. However, the implementation of chatbots can be challenging, as it requires expertise in natural language processing, machine learning, and cloud computing. In this project, we aim to demonstrate the implementation of a serverless chatbot for image moderation, using OpenFaaS and Kubernetes. The chatbot employs multiple serverless functions to handle various tasks, demonstrating the flexibility and scalability of this approach.

The chatbot requires setting up the OpenAI API key in the .env file. We provide you the API key for testing purposes: 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

Github:

[hkust-comp4651-23s/project-discordbot: project-discordbot created by GitHub Classroom](hkust-comp4651-23s/project-discordbot)

Background

OpenFaaS (Functions as a Service) is an open-source framework for building serverless functions using Docker containers. It provides a simple and flexible way to deploy and scale serverless functions, enabling developers to focus on the logic of their functions instead of the infrastructure. Kubernetes is a popular container orchestration platform that provides automated deployment, scaling, and management of containerized applications.

System Design

The discord bot is implemented and deployed in an EC2 instance on AWS. The bot will listen to any incoming traffic in the discord channel and send the message to the OpenFaaS gateway. The OpenFaaS API Gateway routes each request to the appropriate function call. The OpenFaaS deployment is configured with a specified number of replicas, each representing an instance of the function that can handle incoming requests. When a request is received, the OpenFaaS gateway service routes the request to one of the running

replicas. If the incoming request load exceeds the capacity of the running replicas, OpenFaaS can automatically scale up the deployment by creating additional replicas, using Kubernetes Horizontal Pod Autoscaler (HPA) to monitor the CPU usage of the replicas and adjusting the number of replicas based on the defined scaling rules.

Features

The chatbot is able to do the following tasks:
1. Image moderation
2. Text moderation
3. Image generation based on input prompt
4. Chat with user

Image Moderation

To identify photos as Safe for Work (SFW) or Not Safe for Work (NSFW), the image moderation job employs a pre-trained Convolutional Neural Network (CNN) model. The script accepts image upload as input and downloads the picture from the discord cdn server using the urllib2 library. The Caffe library is then used to preprocess and categorize the picture using the NSFW CNN model. The categorization result is outputted by the bot to the channel in a format of the image's SFW and NSFW scores.

Text Moderation

Background of Bert model
BERT, short for Bidirectional Encoder Representations from Transformers, is a Machine Learning (ML) model for natural language processing. It was developed in 2018 by researchers at Google AI Language and serves as a swiss army knife solution to 11+ of the most common language tasks, such as sentiment analysis and named entity recognition

Toxic comment model
The toxic comment model we use is a finetuned version of the Bert model to classify toxic comments. It takes advantage of transfer learning to use the pre-trained Bert model and finetunes with the data from Kaggle Competition https://www.kaggle.com/c/jigsaw-unintended-bias-in-toxicity-classification/data

Image Generation

The image generation task uses the OpenAI API to generate images based on an input prompt. DALL·E model is used in the image generation task. The discord bot listens to any incoming slash commands with the prefix`/image` and `prompt` as the input. It then passes the `prompt` to the OpenFaas serverless function through the OpenFaas gateway. The serverless calls the OpenAI API to generate the image and do any necessary post-processing if any. The serverless function then returns the generated image after processing to the discord bot and the bot will send the image to the discord channel.

Example use case: **/image prompt: a cat sitting on a chair**

Chat

The chat task uses the OpenAI API to generate text based on the most recent 20 chat histories with the user in the channel. GPT3.5-turbo model is used for this task. The discord bot listens to any incoming chat with the prefix `!chat` or any messages inside "chatgpt" text channel. It then passes 100 messages to the OpenFaas serverless function through the OpenFaas gateway. The serverless function filters out only the top 20 chat histories belonging to the bot or the user. OpenAI API is then called to generate the text response and do any necessary post-processing if any. The serverless function then returns the generated text after processing to the discord bot and the bot will send the text to the discord channel. Example use case: **!chat tell me what is 1+1**

Result

Image moderation

The image moderation task demonstrates the effectiveness of the pre-trained CNN model in classifying images as SFW or NSFW. The chatbot provides a simple and efficient way to moderate images using serverless functions, demonstrating the flexibility and scalability of this approach.

safe image

non safe image

wilsonng 今天 16:02

COMP4651 ChatBot 機器人 今天 16:03
dog.jpg is not removed as it has low NFSW score 0.004911927040666342.

COMP4651 ChatBot 機器人 今天 16:13
eve.jpg removed due to displaying explicit or suggestive adult content as it has high NSFW score 0.8786293268203735.

Text moderation

May 4, 2023

Long|Mahiru Today at 8:03 AM
you are a trash dog

May 4, 2023

LongBot BOT Today at 8:03 AM
message by Long|Mahiru#7332 removed due as it is toxic comment

Image Generation

prompt ...

/image prompt An astronaut riding a horse in photorealistic style. 😃

wilsonng 已使用 /image
COMP4651 ChatBot 機器人 今天 16:19

ChatGPT
!chat prefix:

wilsonng 今天 16:15
!chat Do you know about COMP4651 in HKUST?

COMP4651 ChatBot 機器人 今天 16:15
Yes, COMP4651 is a course on Data-intensive Computing at the Hong Kong University of Science and Technology (HKUST). It covers the principles, technologies, and systems for processing and analyzing big data. The course also includes a project component where students will apply the concepts they learn to a real-world problem.

wilsonng 今天 16:16
!chat No, you are wrong, the course title is "Cloud Computing and Big Data Systems"

COMP4651 ChatBot 機器人 今天 16:16
I apologize for the mistake. You are correct, COMP4651 is a course on "Cloud Computing and Big Data Systems" at Hong Kong University of Science and Technology (HKUST). It covers the principles, technologies, and systems for building and deploying cloud-based big data applications. The course covers topics like cloud architecture, big data processing frameworks, data analytics, and distributed systems.

without !chat prefix in chatgpt channel:

wilsonng 今天 16:16
Do you know about COMP4651 in HKUST?

COMP4651 ChatBot 機器人 今天 16:16
Yes! COMP4651 is a course offered by the Hong Kong University of Science and Technology (HKUST), which covers topics related to big data management and processing. It covers topics such as data models, query languages, query processing and optimization, and distributed data processing. Students in this course are expected to have a background in database systems.

wilsonng 今天 16:17
No, you are wrong.
The course title is "Cloud Computing and Big Data Systems"

COMP4651 ChatBot 機器人 今天 16:17
I apologize for the mistake. You are correct that COMP4651 is titled "Cloud Computing and Big Data Systems". The course covers topics such as cloud computing fundamentals, distributed systems, big data processing, storage and data management, real-time data processing, and machine learning. Students in this course are expected to have a background in programming, algorithms, and computer systems.