Oct 23rd, 3:30 PM - 4:00 PM

Developing an AI-Powered Chatbot to Support the Administration of Middle and High School Cybersecurity Camps

Jonathan He
Princess Anne High School, jonathanhe12345678@gmail.com

Chunsheng Xin
Old Dominion University, cxin@odu.edu

Abstract

Throughout the Internet, many chatbots have been deployed by various organizations to answer questions asked by customers. In recent years, we have been running cybersecurity summer camps for youth. Due to COVID-19, our in-person camp has been changed to virtual camps. As a result, we decided to develop a chatbot to reduce the number of emails, phone calls, as well as the human burden for answering the same or similar questions again and again based on questions we received from previous camps. This paper introduces our practical experience to implement an AI-powered chatbot for middle and high school cybersecurity camps using the Google Dialogflow platform.

Location

Zoom Session 1 (Main Papers Track)

Disciplines

Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

A chatbot is a software program that interacts with users in a specific domain or on a particular topic through texts in their natural language (Huang, Zhou & Yang, 2007; Miner et al., 2020). Many chatbots have been deployed on the Internet by various organizations such as governments, banks, hospitals, hotels, and retail stores to answer questions from customers. For example, artificial intelligence-powered chatbots have been provided by the World Health Organization to provide information regarding the spread of the coronavirus disease and its symptoms (Martin et al., 2020; Espinoza et al., 2020).

Generally, an online chatbot provides a textbox for a user to enter a question to comment. Based on the information provided by the user, the chatbot will find relevant answers to the subject and respond to the user through a dialog form. Herriman et al. (2020) summarized two main benefits of chatbot including: 1) chatbots are available online anytime and allow people to immediately obtain answers or information 24/7 instead of having to wait for a human to provide information; 2) Chatbots can serve many users simultaneously and provide consistent solutions to frequently asked questions. Sundareswaran and Firth-Butterfield (2020) also point out that chatbots presents an intuitive approach to disseminate curated information and can offer a response to specific questions in an interactive manner.

In recent years, we have been running cybersecurity summer camps for youth to combat the current problem of the shortage of workforce for cybersecurity professionals. The goals of the camps are to increase youth's interest in cybersecurity careers and help students understand correct and safe online behavior. Moreover, they can learn how to become good digital citizens and learn various hands-on cybersecurity skills such as setting up a firewall, learning to analyze network traffic, and cracking passwords.

So far, our camps have taught cybersecurity knowledge and skills to hundreds of middle and high school students and developed their interest in learning more about cybersecurity. We usually start advertising our planned camps two or three months before the camp's starting date. We received many questions regarding cybersecurity content and topics, as well as camp logistics from students, parents, and schoolteachers before, during, and after camps. Many of the questions we received are repetitive or similar questions and can be answered by the chatbots. Due to COVID-19, we must change our face-to-face camps to virtual camps for the year 2020 and possibly the next few years. Therefore, we decided to develop a chatbot based on previous questions we received to reduce the number of emails, phone calls as well as the human burden for answering the same or similar questions again and again. We selected some frequently asked questions for building our

chatbot. Instead of posting many frequently asked questions directly on the website, which many people may not be interested in reading, we feel that chatbots can be a good alternative and provide responses to any user's questions or inquiries in an interactive manner. Section 2 describes the process we followed to develop the chatbot.

CHATBOT BUILDING

Modern chat robots are mainly divided into rule-based chatbots and AI-based chatbots (Maroengsit et al., 2019). The rule-based chatbots primarily use numerous If-Else statements to filter the question-answer pairs. In contrast, the AI-based chatbots use a repository of predefined responses and some heuristic methods to select the appropriate response based on input and context. Developing AI-based chatbots is challenging because computers traditionally only understand a programming language that is precise, unambiguous, and highly structured. Different from programming languages, human languages are often ambiguous and complicated which include slang, regional dialects, and social context. The key solution is to utilize complex machine learning classifier sets and AI techniques to converse with users. Further, AI-based chatbots can be categorized using two approaches: retrieval-based and generative-based (Maroengsit et al., 2019). Retrieval-based approach searches a user-issued query from a database and returns a reply that best matches the query (Song et al., 2016). When the database is small, it may not find a reply. In contrast, generative-based approach often uses recurrent neural networks to generate new responses, but it could generate meaningless responses (Song et al., 2016). Both approaches have their strengths and weaknesses. In our case, we adopted a retrieval-based approach as it works best for goal-oriented bots in customer support, lead generation, and feedback. We list the steps of our implementation of the chatbot as below:

1) Incorporating selected questions

Producing a reasonable response system needs to incorporate specific questions and linguistic context. The questions we selected are from three sources including the most frequently asked questions we received from emails in previous years, common questions students asked during the camps, as well as some common questions we selected from several online cybersecurity resource websites and discussion forums (Huang et al., 2007). For each question, we collaborated to provide several training phrases consisting of different ways a person might ask or phrase a question. Based on these questions, we also found out its linguistic context one by one, and gradually induced the preconditions of that context.

2) Developing possible responses to the selected questions

Based on each of the selected questions and context, we developed specific responses using the information we have about our camps, relevant technical documents, and resources from the Internet. We discussed those responses to produce consistent answers to semantically identical inputs. Moreover, we made redundant and diverse responses to make the chatbot more personal. Appropriate responses will be returned to the user after the chatbot internally matches the response with specific questions the user asked. The response can have several types, including an answer to a particular question (if available), ask the user to clarify or provide more information, or say goodbye (ending the chat). If a question cannot be answered, the chatbot can share a website or contact phone number with the user or escalate the question to the summer camp staff for further processing. A challenge of developing an effective chatbot is that it could be hard to develop a large initial set of possible questions and good answers for training purpose.

3) Creating a chatbot using Google Dialogflow

We developed the chatbot using Google Dialogflow, which is a natural language understanding platform provided by Google as a service that runs on Google Cloud Platform (Dialogflow, 2020). Dialogflow allows developers to quickly design and create conversational interfaces or chats across devices and platforms using Dialogflow Console, which also provides functions to help developers integrate the chatbot with websites, mobile apps, or social media sites. Dialogflow leverages Google's strength in natural language processing and machine learning to generate and train natural language models for processing user input (Reyes et al., 2019). As a result, Dialogflow can map diverse questions from users to relevant underlying intents, which are the motivation behind a user input. Figure 1 shows the Google Dialogflow Console Interface with an example containing training phrases related to summer camp cost-related questions as well as possible responses.

Google Dialogflow can recognize many more phrases after training using the initial small training set consisting of a few training phrases provided by developers. Chatbots built by Google Dialogflow can respond to users using text or voice-based speech. Dialogflow also provides an API to create intents using data extracted from backend databases. Dialogflow has been used by developers in companies such as BestBuy and Ticketmaster to build voice- and text-based chatbots powered by machine learning and natural language understanding (Greig, 2018).

We entered the questions and responses from Step 1 and 2 using Dialogflow Console and built multiple intents and entities to generate appropriate responses to the user's queries. It took us some time to create a fully functional chatbot through trial and error, and rounds of refinement. Figure 2 shows the essential procedures that explain how a chatbot matches responses with questions internally.

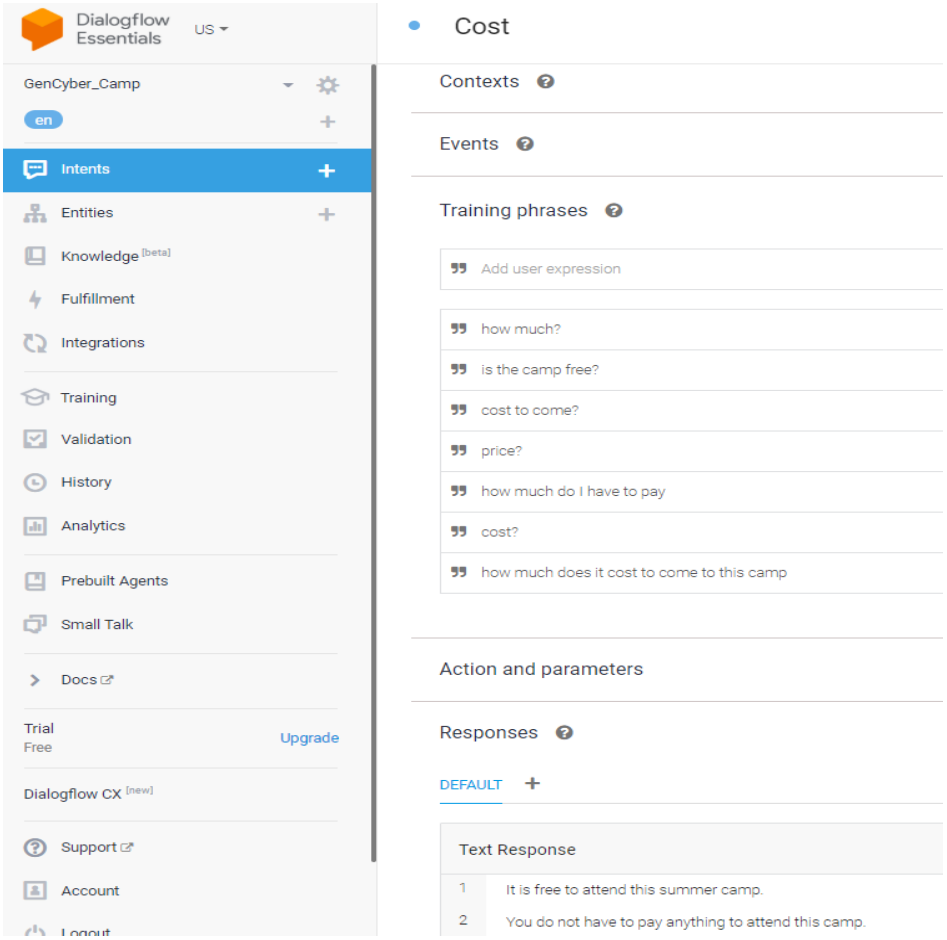

Figure 1. Google Dialogflow Console Interface

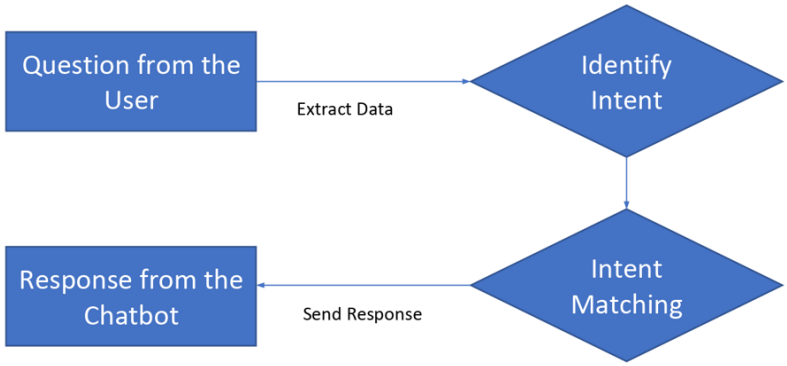

Figure 2. How to implement a chatbot internally using Google Dialogflow

4) Deploying the chatbot on our summer camp website

Dialogflow provides multiple integration options to help developers easily integrate the developed chatbot with websites as well as many popular conversation platforms, including Google Assistant, and Facebook Messenger. We decided to incorporate the developed chatbot with our summer camp website directly so that any visitors to our website can interact with the chatbot and ask questions as needed. Visitors can chat with this chatbot and get responses on questions such as summer camp logistics, basic cybersecurity concepts, emergency contact, and so on. Figure 3 shows the user interface of our developed chatbot.

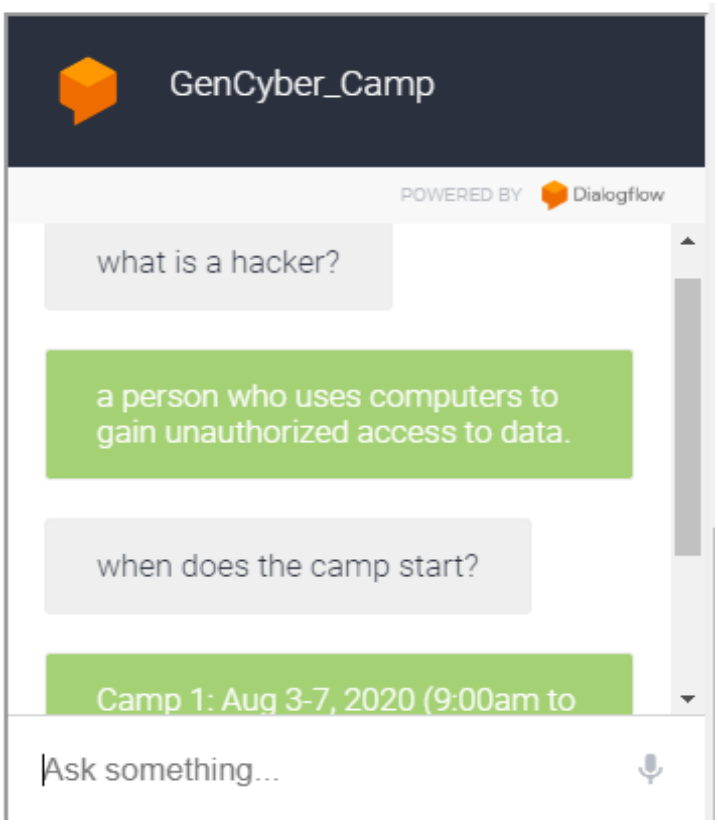

Figure 3. User interface of the chatbot

Our preliminary evaluation of the chatbot shows that the chatbot was well received by those who used it. 29 students filled out a short questionnaire after they used the chatbot. 79.5% of the students agreed that the chatbot was easy to use; 89.6% of them agreed that the chatbot's interface was user-friendly; 89.7% of them thought the chatbot works great and the chatbot was very helpful and helped them answer some of their camp or cyber related questions; 75.9% of them enjoyed

using the chatbot; Overall, 82.8% of then were satisfied with the chatbot. Based on the feedback, we further changed the font color of the response to the questions to differentiate the questions and responses.

5) Maintaining the chatbot

To make chatbots more useful to others, chatbots should be updated on an ongoing basis to incorporate new questions asked by users through the chatbot or other channels over time. Chatbots can become outdated later if no further questions/responses are added to the chatbot, and people will stop using it if they feel the chatbot cannot keep up with the change over time. Chatbots should be trained regularly as new training phrases are being included in the chatbot (Herriman et al., 2020) to achieve better accuracy and variability of language.

Google Dialogflow provides an analytics function to show usage data statistics, including various user requests and response data statistics over time. We can easily use these data statistics to assess the usage of the developed chatbot, identify new questions from the chat records, and find ways to improve the chatbot.

CONCLUSION

Chatbots are a low-cost tool that can be developed and deployed rapidly to support many online users simultaneously. More and more businesses and organizations are deploying chatbots on their websites and social media platforms to assist customers or users.

We believe that a chatbot can be more useful than a Q&A agent and it can be further developed to become an advanced virtual assistant for both teachers and students. As for future work, we are interested in expanding the chatbot for general questions in the cybersecurity area so that the chatbot can provide standardized answers to more knowledge-related questions about cybersecurity. If well implemented, this chatbot can be used to serve thousands of students simultaneously, which will be very useful to numerous students who are learning cybersecurity worldwide (Reyes et al., 2019).

REFERENCES

Dialogflow(2020). Create conversational experiences across devices and platforms. Available at https://cloud.google.com/dialogflow/

Greig, J. (2018). Google's Dialogflow Enterprise helps businesses create AI-powered chatbots. Available at https://www.techrepublic.com/article/google-officially-unveils-chatbot-

dialogflow-enterprise/

Herriman, M, Meer, E., Rosin, R., Lee, V., Washington, V, & Volpp, K. (2020). Asked and Answered: Building a Chatbot to Address COVID-19-Related Concerns. *NEJM Catalyst Innovations in Care Delivery*. DOI: 10.1056/CAT.20.0230.

Huang, J., Zhou, M., & Yang, D. (2007). Extracting Chatbot Knowledge from Online Discussion Forums. In *IJCAI*(Vol. 7, pp. 423-428).

Maroengsit, W., Piyakulpinyo, T., Phonyiam, K., Pongnumkul, S., Chaovalit, P., & Theeramunkong, T. (2019, March). A Survey on Evaluation Methods for Chatbots. In *Proceedings of the 2019 7th International Conference on Information and Education Technology* (pp. 111-119).

Martin, A., Nateqi, J., Gruarin, S., Munsch, N., Abdarahmane, I., & Knapp, B. (2020). An artificial intelligence-based first-line defence against COVID-19: digitally screening citizens for risks via a chatbot. *bioRxiv*.

Reyes, R., Garza, D., Garrido, L., De la Cueva, V., & Ramirez, J. (2019). Methodology for the Implementation of virtual assistants for education using Google Dialogflow. In *Mexican International Conference on Artificial Intelligence* (pp. 440-451). Springer, Cham.

Sundareswaran, V & Firth-Butterfield, K. (2020). Chatbots provide millions with COVID-19 information every day, but they can be improved - here's how. Available at https://www.weforum.org/agenda/2020/04/chatbots-covid-19-governance-improved-here-s-how/

Song, Y., Yan, R., Li, X., Zhao, D., & Zhang, M. (2016). Two are better than one: An ensemble of retrieval-and generation-based dialog systems. *arXiv preprint arXiv:1610.07149*.