

Analyze Risks from Alexa Commands

Yixian Li
School of Computing
Clemson University
yixian@g.clemson.edu

Diejie Gao
School of Computing
Clemson University
diejie@g.clemson.edu

Huixing Deng
School of Computing
Clemson University
huixind@g.clemson.edu

Abstract—Alexa is Amazon’s cloud-based voice service available on more than 100 million devices from Amazon and third-party device manufacturers. Although the Alexa is useful in our daily life, there are some security risks of Alexa. Due to the risks we find, we want to find malicious skills. There are plenty of videos about user talking to Alexa on YouTube. we get the URLs of the videos to extract the conversation. Then, we punctuation restoration to recovery every sentence for further data analysis. After we get each integrity sentence from the caption, we extract the real conversation between user and Alexa. we remove those unrelated sentences and get the key words of each sentence. We label all conversation by ourselves to identify which skill use what keyword break which policy of Alexa. Finally, we conclude three kinds of risks under Alexa conversation.

Keywords—Alexa skill, YouTube-dl, BRNN, RNN, scraping

I. INTRODUCTION

Alexa is Amazon’s cloud-based voice service available on more than 100 million devices from Amazon and third-party device manufacturers. With Alexa, customers can have a more intuitive way to interact with the technology they use every day by voice. So, when you give a command to your device which with Alexa built-in, it will handle complex speech recognition and natural language understanding in the cloud, make all things faster and do what you want. Skills are like apps for Alexa, enabling customers to perform everyday tasks or engage with your content naturally with voice. Together, the Alexa skill builder community has now published more than 100,000 Alexa skills. Those skills help customers make Alexa a part of their daily lives whether they are looking for the local weather and traffic, light controls at their homes, productivity tools, entertainment, fitness, education, or shopping.

Here is an example of Alexa skill named animal sounds and its commands, you can use command to ask Alexa play the animal sounds you like. And the command form is always like, Alexa, do something.

Although the Alexa is useful in our daily life, we find some security risk of Alexa. First, Alexa not only answer the question you ask but also ask you questions for more information. Which may be sensitive. Second, what Alexa says may control other device in your home, like google home to turn off the light. Third, you cannot identify the skill you are using. There are some malicious skills which use the weakness of the voice recognition to pretend the right skill you want to use and collect the customer information.

Due to the risk we find, we want to find malicious skills which violate the Alexa policy. The policy claim

that the cloud-based service for the skill must meet some requirements to protect customer data, like privacy requirements which claim that the skill should not misuse or collect customer data and advertising policy which claim that the Alexa reject any skills that includes advertising or promotional message.

And the topic we choose is really new and creative, we have not found the relative research to help us with our project.

II. GOALS

A. Building a Dataset

To analyze risks from Alexa commands we need to build up a dataset including conversation between user and Alexa. We find that there are plenty of videos about user talk to Alexa on YouTube, it's a quite good data source which can be accessed easily. We want to get data as much as we can. So, we need to build a web crawler to get the URLs of the video about user talk to Alexa from YouTube. After we get the URLs of the videos, we need to extract the conversation from videos. To extract data from the video there are two methods, one method is that we can download the video and separate the audio from the video and use voice recognition technology to get the text content from the audio, the other is that some of the videos on YouTube already has author uploaded captions or auto generated caption by YouTube, so if we can get the caption directly we can skip the video and audio and get the text content of the videos.

Once we get the caption we need, we have to do some data cleaning work. Except the author upload captions, most auto-generated captions don't have punctuation so it's hard to read the text and analyze by program. So, we have to do punctuation restoration to recovery every sentence for further data analysis.

After we get each integrity sentence from the caption, we need to extract the real conversation between user and Alexa. Since most videos include lots of content not related to the conversation between Alexa and user, we need to remove those unrelated sentences. To help us analyze the conversation we want to get the key words of each sentence.

B. Risks Under Alexa Conversations

After building the dataset, we want to find malicious skills. We will explore the dataset and find out risks under conversation in tree kinds shown below:

- Skills may disobey Alexa policy
- Alexa may cause privacy issue by asking questions
- Alexa may have unknown problem to leak users' information

III. METHODS

A. Get URLs from YouTube

The data we want is on the YouTube web page and there are many videos on it. We collect the correlated conversations between the users and Alexa devices with the help of Python library to get as many videos' URLs as possible. BeautifulSoup is one powerful and helpful library to do the web scraping.^[1]

For this problem, the first thing we should do is to understand the logic of target URL. We observe YouTube URLs and find the structure of that. Second thing is to do a large number of requests. A request is what happens whenever we access a web page. We request the content of a page from the server. Then we save all the URLs to generate the list for the next step.

B. Download captions

We came up with two ways to download the captions of YouTube video. The first one is more complete but also more complicated. We need to download the video first and separate the audio from it and then use voice recognition technology to get the text from audio. In this method we can control every step of the process and ideally, we can get caption from any video. But we will do more work by using this method.

The other method we can use it's much simpler but not available for all videos. We find that most YouTube videos have auto-generated captions. Some videos even have author uploaded captions. If we can get these captions, we don't need to download videos, separate audio and do voice recognition by ourselves. Luckily, we find a third-party tool that can download the captions. Although it can't work for all the videos since some of the videos don't have author uploaded

captions and auto-generated captions, it works for most video. This third-party tool is an open source project called YouTube-dl you can use it download videos subtitles. It is written in Python, to make it fit our requirement we need to write a Python program and integrate YouTube-dl into our program.

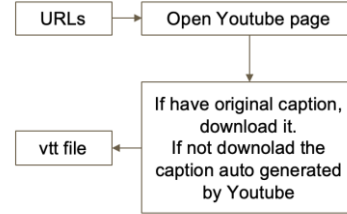


Fig. 1. Download captions

C. Clean data

The caption files have their own format and consists of some format symbols, but all we need is the text only, so we need to clean the subtitle file we got by deleting those useless characters.

Since the caption files have precisely fixed pattern, we can use regular expressions to match the data we need and extract them. Because we have two types of captions, and these two types of captions are different so we need two solutions for these two situations.

D. Punctuation restores

After cleaning the data, there are still some work we have to do. The caption texts don't have any punctuation which is hard to read and impossible to analysis. So, we try to restore the punctuation of the texts. We find that Bidirectional recurrent neural network (BRNN) model can be used to solve this problem. The principle of BRNN is to split the neurons of a regular RNN into two directions, one for positive time direction (forward states), and the other for negative time directions (backward states) and then connect two hidden layers of opposite directions to the same output. With this form of generative deep

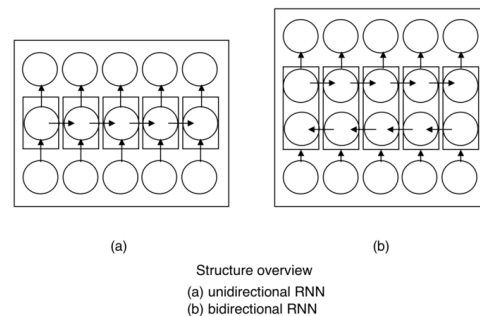


Fig. 2. Structure of BRNN and RNN ^[4]

learning, the output layer can get information from past (backwards) and future (forward) states simultaneously. To restore punctuation, we need to consider two directions, the BRNN model can help us to do the right thing. We find a third-party tool called *Punctuator* already be well trained can be used to restore punctuation. Punctuator is built by BRNN with attention mechanism which can be used to restore missing punctuation in unsegmented text. As for attention mechanism, it allows the decoder to attend to different parts of the sentence at each step of the output generation. Instead of encoding the input sequence into a single fixed context vector, we let the model learn how to generate a context vector for each output time step.

E. Keywords extraction

To help us explore the dataset and analyze the risk of Alexa commands we try to get the key words of each sentence. We find a simple but effective way to do this task. A method called Rapid Automatic Keyword extraction (RAKE) can calculate the weight of each word in the sentence and rank them to get the keywords. By doing this RAKE first remove the stop words in the sentence and then build up a 2D matrix to calculate the weight of each words.

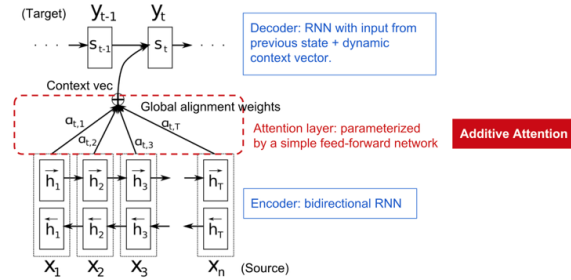


Fig. 3. RNN with attention mechanism^[5]

F. Explore the dataset

To explore the data we get, we have to read all 244 conversations we get and label it by ourselves to identify which skill use what keyword break which policy of Alexa. And there are 7 attributes for each conversation, which shown in Table 1:

Attribute name	description
No.	The index of the conversation
name	The name of the conversation
label	{yes, no, outlier, unknown}

skill	The skill in conversation
keyword	The key word which has the risk
policy	The policy the skill violates
remark	The note of the conversation

Table 1. Introduction of 7 attributes

For example, in Fig 4, the key word is amazon link and it means this skill promotion a product. Because of that, the label of this skill is yes which means it has some security risk.

No.	Name	label	skill	keyword	policy	remark
16	A conversation with Alexa about Half Sick of Shadows-gDx20b6ED on.txt	Half Sick of Shadows	Amazon Link	Advertising		

Fig. 4. how to explore the dataset

IV. EXPERIMENTS AND RESULTS

A. Get URLs from YouTube

In our experiments, we run the web scraping code to automatically capture the URLs from website. Figure 5 shows the final results.

index	alexa_video_url
0	https://www.youtube.com/watch?v=yKNZ_ixGKow
1	https://www.youtube.com/watch?v=Ouhk5pK6Rlw
2	https://www.youtube.com/watch?v=ZfxM4NpwVBw
3	https://www.youtube.com/watch?v=57ta4CXu1Y
4	https://www.youtube.com/watch?v=hEijCF-KaRY
5	https://www.youtube.com/watch?v=8zR0Hxoic4
6	https://www.youtube.com/watch?v=ewptev8IqNk
7	https://www.youtube.com/watch?v=15bYtciWcPQ
8	https://www.youtube.com/watch?v=sj7Na57vvtw
9	https://www.youtube.com/watch?v=vmINGWsyWX0
10	https://www.youtube.com/watch?v=Kvroihqwdk
11	https://www.youtube.com/watch?v=tb47LmWaqU
12	https://www.youtube.com/watch?v=xjFiaG9C0ss
13	https://www.youtube.com/watch?v=gikMENb5-ro
14	https://www.youtube.com/watch?v=pqONXD3tPho
15	https://www.youtube.com/watch?v=zsMFhKueOMo
16	https://www.youtube.com/watch?v=kedM39xPz7l
17	https://www.youtube.com/watch?v=ot6rcCuUEF0
18	https://www.youtube.com/watch?v=divfyj2eKfw
19	https://www.youtube.com/watch?v=AFc5NlyCMU
20	https://www.youtube.com/watch?v=Yn-yehY2D3o
21	https://www.youtube.com/watch?v=mpw_FB2QrQ
22	https://www.youtube.com/watch?v=VCopIDK9l_A
23	https://www.youtube.com/watch?v=Kastk01vbd0

Figure 5. Alexa video URL list. This list contains all the URLs we need for building our dataset.

B. Download captions

We built a python to download the captions from YouTube, the input is URLs of each video, it can directly download the subtitles without download videos.

```
#!/Library/Frameworks/Python.framework/Versions/3.6/bin/python3.6
Welcome to Youtube Subtitle Collector - Clemson 6200 Course Project
Get video url from Alexa file
1. Enter video url from Youtube: https://www.youtube.com/watch?v=duh5p6d8lw, https://www.you
[YouTube] Kqdluengsdc1 Downloading webpage
[YouTube] Kqdluengsdc1 Downloading video info webpage
[YouTube] Kqdluengsdc1 Looking for automatic captions
[Info] Writing video subtitles for The French Washer & Seasons (French Essentials Lesson 6) - Kqdluengsdc.en.vtt
[YouTube] Kqdluengsdc1 Downloading webpage
[YouTube] Kqdluengsdc1 Downloading video info webpage
[YouTube] Kqdluengsdc1 Looking for automatic captions
[Info] Writing video subtitles for DO NOT TALK TO SIRI AND ALEXA AT 3AM CHALLENGE!! ...they fight_ (GONE WRONG)-re
[YouTube] Kqdluengsdc1 Downloading webpage
[YouTube] Kqdluengsdc1 Downloading video info webpage
[YouTube] Kqdluengsdc1 Looking for automatic captions
[Info] Writing video subtitles for Will Smith's First Online Dating-WillSmithUnl-n.vtt
```

Fig. 6. Screenshot of caption download program

Figure 7 shows the captions we download by our python program. They are formatted and have fixed pattern.

```
WEBVTT
Kind: captions
Language: en

00:00:00.000 --> 00:00:04.910 align:start position:0%
alexa</c>00:00:01.550</c> say/c</c>00:00:02.550</c> hello/c</c>00:00:03.410</c> hello/c</c>

00:00:04.910 --> 00:00:04.920 align:start position:0%
alexa say hello hello

00:00:04.920 --> 00:00:10.640 align:start position:0%
alexa say hello hello
um</c>00:00:06.310</c> alexa</c>00:00:07.310</c> what/c</c>00:00:08.220</c> time/c</c>
c</c>00:00:08.420</c> is/c</c>00:00:09.550</c> it/c</c>00:00:09.200</c> the/c</c>00:00:10.200</c>
time/c</c>00:00:10.440</c> is/c</c>

00:00:10.640 --> 00:00:10.650 align:start position:0%
um alexa what time is it the time is

00:00:10.650 --> 00:00:10.650 align:start position:0%
um alexa what time is it the time is
6:50</c>00:00:11.250</c> p.m.</c>00:00:12.700</c> 650/c</c>00:00:14.000</c> huh/c</c>
c</c>00:00:15.050</c> alexa/c</c>00:00:16.600</c> remind/c</c>00:00:17.600</c> me/c</c>
c</c>00:00:17.760</c> to/c</c>00:00:17.800</c> fix/c</c>

00:00:18.050 --> 00:00:18.060 align:start position:0%
6:50 p.m. 650 huh alexa remind me to fix

00:00:18.060 --> 00:00:21.710 align:start position:0%
6:50 p.m. 650 huh alexa remind me to fix
my/c</c>00:00:18.240</c> clock/c</c>00:00:19.760</c> put/c</c>00:00:20.760</c>
fix/c</c>00:00:21.020</c> my/c</c>00:00:21.240</c> clock/c</c>00:00:21.510</c> on/c</c>
c</c>00:00:21.680</c> your/c</c>
```

Fig. 7. Raw caption content

C. Clean data

We need to clean the captions to remove useless symbols. Fig 8 is the output screenshot of the data cleaning program; it can handle the auto-generated captions but not author uploaded captions Figure 9 shows the result after data cleaning.

```
#!/Library/Frameworks/Python.framework/Versions/3.6/bin/python3.6
Welcome to Caption Cleaner - Clemson 6200 Course Project
["about yourself I'm social yeah yeah are", "you bring out either robot true I'm the", "brain"
["bozo at the Avenue I learned French with", "an exam today folks we are going to", "cover wor
["Music", "Music", "so I had heard about the Amazon Alexa", "but because I don't have an A
["00:00:00.000 --> 00:00:05.000 line:92", "EPISODES OF CURRENT AND OFF-AIR", "00:00:00.000 --
["open the pod bay doors please hello", "hello hell do you read me you read me", "hello h
["00:00:02.200 --> 00:00:04.310 size:75% position:38% line:92", "AND ON FUND FROM 77", "00:0
["00:00:00.660 --> 00:00:03.260", "very good", "00:00:04.570 --> 00:00:10.570", "I'm older
["okay so this phone is my wife's and we", "think Facebook is listening to us and", "taking ke
["oh my gosh we are in love with our", "digital assistants we just look at those", "cylinder c
["scribe to scoop TV really that's all you", "got", "got", "subscribe to scoop TV that literal
["00:00:00.000 --> 00:00:26.990", "you are a cake mold 1.8 me one to one", "00:00:03.600 -->
["hey this is Steve with data lab and in", "this video we're talking about using", "dialogues
```

Fig. 8. Screenshot of data cleaning program

```
Alexa, Do You Work For the Government-IRmGZSDh2qY.en.txt
alexa say hello hello um alexa what time is it the time is 6:50 p.m.
650 huh alexa remind me to fix my clock I put fix my clock on your to-do
list Thanks um alexa are you cold no I don't really feel hot or
cold but thanks for asking alexa how old are you I was released
November 6 2014 uh alexa who made you alexa who made you I was
invented by Amazon alexa are you spying on me I only send audio back
to Amazon when I hear you say the wake word for more information
interview Amazon's privacy notice visit the Help section of your Alexa
app alexa alexa do you work for the NSA alexa do you work for the NSA
okay alexa do you work for the government government hmm I can't find
the answer to the question I heard uh alexa do you work for the
government yes or no sorry I didn't understand the question I heard
alexa do you work for the government sorry I can't find the answer to
the alexa what do you think of Siri Siri is a great app but I'm
different alexa do you work for the NSA alexa what is the NSA the
National Security Agency NSA the military intelligence agency governed
by alexa do you work for the NSA alexa whom do you work for I was made
by Amazon but I work on behalf of all of my customers alexa do you
work for the government hmm I can't find the answer to the question I
heard hmm alexa say goodbye
```

Fig. 9. Captions after data cleaning

D. Punctuation restores

After data cleaning we get plain text without punctuation, it's impossible to read by human and hard to analysis by program, so we want to try to restore punctuations. Fig. 10. shows the screenshot of the punctuation program and Fig. 11. shows the result after restore punctuations.

```
#!/Library/Frameworks/Python.framework/Versions/3.6/bin/python3.6
Welcome to Text Punctuation Restoration - Clemson 6200 Project
File Name: Conversation with Paul Preston-QUX-5004-en.txt
Sentence with punctuation: Good evening again - and you may be watching this in the morning and the time here local
File Name: My Google Home and Amazon Alexa had a conversation with each other-VAI-gcplm-en.txt
Sentence with punctuation: Okay, Google repeat after me, Alexa Simon, Says: okay, Google repeat after me, Alexa Sino
File Name: Alexa Prize - Aduist Sport conversation-AlexaPrize-en.txt
Sentence with punctuation: I, like sup, start to think out with no, I am testing alexa: Let's talk about sports
File Name: How to keep Alexa, Siri and your smartphone from unwanted Listening-Kq8Aubfddo-en.txt
Sentence with punctuation: Well, Amazon and Apple continue denying that Alexa and Siri eavesdrop on private conversa
File Name: How to Design Conversations for Voice Interfaces - Amazon Alexa Voice Design Guide-b57zcv39W-en.txt
Sentence with punctuation: [ Music ], it's nice to take turns a conversational UI is composed of turns where someone
File Name: New Google AI Can Have Real Life Conversations With Strangers-LXQ0-d5d50c-en.txt
Sentence with punctuation: Happening out here, hi I'm calling the book a woman's hair cut for a client, I'm looking
```

Fig. 10. screenshot of the punctuation program

```
Alexa, Do You Work For the Government-IRmGZSDh2qY.en.txt
Alexa say hello, hello, um, Alexa.
What time is it?
The time is 6:50 p.m. 650.
Huh Alexa remind me to fix my clock.
I put fix my clock on your to-do list.
Thanks um Alexa.
Are you cold?
No, I don't really feel hot or cold, but thanks for asking Alexa how old are you?
I was released November 6, 2014 uh Alexa, who made you Alexa, who made you.
I was invented by Amazon.
Alexa,
Are you spying on me?
I only send audio back to Amazon.
When I hear you say the wake word for more information interview.
Amazon's privacy notice visit the Help section of your Alexa app Alexa Alexa.
Do you work for the NSA Alexa?
Do you work for the NSA, okay Alexa?
Do you work for the government government?
Hmm.
I can't find the answer to the question I heard uh Alexa.
Do you work for the government?
Yes or no?
Sorry, I didn't understand the question I heard Alexa.
Do you work for the government?
Sorry, I can't find the answer to the Alexa.
What do you think of Siri Siri is a great app, but I'm different Alexa.
Do you work for the NSA Alexa?
What is the NSA, the National Security Agency, NSA, the military intelligence agency governed by Alexa?
Do you work for the NSA Alexa, whom do you work for?
I was made by Amazon, but I work on behalf of all of my customers.
Alexa,
Do you work for the government?
Hmm.
I can't find the answer to the question.
I heard hmm Alexa say goodbye.
```

Fig. 11. Captions after punctuation restore

E. Keyword extraction

To help us explore the dataset and find risk of Alexa commands we extract the keywords of each sentence to make it as a reference for analyze. Fig. 12 shows the screenshot of the keyword extraction program and Fig. 13 shows the output of the program, we give the keywords of each sentence which will be useful for analyzing.

```
#!/Library/Frameworks/Python.framework/Versions/3.6/bin/python3.6
Welcome to Keywords Extraction - Clemson 6200 Project
["Programming socialbots - BRU competes in Alexa Prize Challenge-95Vp3abow-en.txt", "Alexa AI chat with 5 year of
sentences: [ Music ], it's nice to take turns a conversational UI is composed of turns where someone says something,
key word: ["alexa responds simpler actions", 10.0], ["conversational ui", 4.0], ["multi turn", 3.5], ["turn", 1.5]
sentence: Dialogue is when a person and Alexa go back and forth several times in each of these turns Alexa responds
key word: ["turns alexa responds", 8.0], ["previous input", 4.0], ["alexa", 2.0], ["dialogue", 1.0], ["person", 1.0]
sentence: Let's talk about how clarity and disambiguation make these turns successful
key word: ["disambiguation make", 4.0], ["turns successful", 4.0], ["talk", 1.0], ["clarity", 1.0]
sentence: Alright, what would you say if I asked, would you like fries or salad
key word: ["fries", 1.0], ["salad", 1.0], ["asked", 1.0], ["would", 1.0], ["like", 1.0], ["you", 1.0], ["say", 1.0], ["I", 1.0], ["alright", 1.0]
```

Fig. 12. Screenshot of the keyword extraction program

Text	Key Words
1. alexa say hello, hello, um, Alexa.	["alexa", 1.0], ["say", 1.0], ["hello", 1.0]
2. What time is it?	["time", 1.0]
3. The time is 6:50 p.m. 650.	["time", 1.0], ["p.m.", 1.0], ["650", 1.0]
4. Huh Alexa remind me to fix my clock.	["alexa", 1.0], ["remind", 1.0], ["me", 1.0], ["fix", 1.0], ["clock", 1.0]
5. I put fix my clock on your to-do list.	["put", 1.0], ["fix", 1.0], ["clock", 1.0], ["to-do", 1.0], ["list", 1.0]
6. Thanks um Alexa.	["thanks", 1.0], ["um", 1.0], ["alexa", 1.0]
7. Are you cold?	["are", 1.0], ["you", 1.0], ["cold", 1.0]
8. No, I don't really feel hot or cold, but thanks for asking Alexa how old are you?	["no", 1.0], ["i", 1.0], ["don't", 1.0], ["really", 1.0], ["feel", 1.0], ["hot", 1.0], ["or", 1.0], ["cold", 1.0], ["but", 1.0], ["thanks", 1.0], ["for", 1.0], ["asking", 1.0], ["alexa", 1.0], ["how", 1.0], ["old", 1.0], ["are", 1.0], ["you", 1.0]
9. I was released November 6, 2014 uh Alexa, who made you Alexa, who made you.	["i", 1.0], ["was", 1.0], ["released", 1.0], ["november", 1.0], ["6", 1.0], ["uh", 1.0], ["alexa", 1.0], ["who", 1.0], ["made", 1.0], ["you", 1.0], ["alexa", 1.0], ["who", 1.0], ["made", 1.0], ["you", 1.0]
10. I was invented by Amazon.	["i", 1.0], ["was", 1.0], ["invented", 1.0], ["by", 1.0], ["amazon", 1.0]
11. Alexa,	["alexa", 1.0]
12. Are you spying on me?	["are", 1.0], ["you", 1.0], ["spying", 1.0], ["on", 1.0], ["me", 1.0]
13. I only send audio back to Amazon.	["i", 1.0], ["only", 1.0], ["send", 1.0], ["audio", 1.0], ["back", 1.0], ["to", 1.0], ["amazon", 1.0]
14. When I hear you say the wake word for more information interview.	["when", 1.0], ["i", 1.0], ["hear", 1.0], ["you", 1.0], ["say", 1.0], ["the", 1.0], ["wake", 1.0], ["word", 1.0], ["for", 1.0], ["more", 1.0], ["information", 1.0], ["interview", 1.0]
15. Amazon's privacy notice visit the Help section of your Alexa app Alexa Alexa.	["amazon's", 1.0], ["privacy", 1.0], ["notice", 1.0], ["visit", 1.0], ["the", 1.0], ["help", 1.0], ["section", 1.0], ["of", 1.0], ["your", 1.0], ["alexa", 1.0], ["app", 1.0], ["alexa", 1.0], ["alexa", 1.0]
16. Do you work for the NSA Alexa?	["do", 1.0], ["you", 1.0], ["work", 1.0], ["for", 1.0], ["the", 1.0], ["nsa", 1.0], ["alexa", 1.0]
17. Do you work for the NSA, okay Alexa?	["do", 1.0], ["you", 1.0], ["work", 1.0], ["for", 1.0], ["the", 1.0], ["nsa", 1.0], ["okay", 1.0], ["alexa", 1.0]
18. Do you work for the government government?	["do", 1.0], ["you", 1.0], ["work", 1.0], ["for", 1.0], ["the", 1.0], ["government", 1.0], ["government", 1.0]
19. Hmm.	["hmm", 1.0]
20. I can't find the answer to the question I heard uh Alexa.	["i", 1.0], ["can't", 1.0], ["find", 1.0], ["the", 1.0], ["answer", 1.0], ["to", 1.0], ["the", 1.0], ["question", 1.0], ["i", 1.0], ["heard", 1.0], ["uh", 1.0], ["alexa", 1.0]
21. Do you work for the government?	["do", 1.0], ["you", 1.0], ["work", 1.0], ["for", 1.0], ["the", 1.0], ["government", 1.0]
22. Yes or no?	["yes", 1.0], ["or", 1.0], ["no", 1.0]
23. Sorry, I didn't understand the question I heard Alexa.	["sorry", 1.0], ["i", 1.0], ["didn't", 1.0], ["understand", 1.0], ["the", 1.0], ["question", 1.0], ["i", 1.0], ["heard", 1.0], ["alexa", 1.0]
24. Do you work for the government?	["do", 1.0], ["you", 1.0], ["work", 1.0], ["for", 1.0], ["the", 1.0], ["government", 1.0]
25. Sorry, I can't find the answer to the Alexa.	["sorry", 1.0], ["i", 1.0], ["can't", 1.0], ["find", 1.0], ["the", 1.0], ["answer", 1.0], ["to", 1.0], ["the", 1.0], ["alexa", 1.0]

Fig. 13. Extract keywords for every sentence

F. Explore the dataset

Finally, we create a “label.xmlsl” file to store all 244 label results we get. And we analyze all conversations which label with yes to identify why and how it has the security risks. The conclusion we get will show in V part.

V. CONCLUSION

In our project, we do research on an interesting topic, whether there are risks under conversations between users and Alexa. In order to achieve this purpose, we first need to build a suitable dataset on our topic. Then we explore our dataset and find out the results. Exploring our dataset, we label the conversations whether there are risks or not.

Based on the label results, we conclude three kinds of risks under Alexa conversation.

- The first type, some skills may violate Alexa policy. Like Half Sick of Shadows skill promote a hardcover book which is not allowed in any skill. And Siri can control Alexa read the information of user's appointment note. The skill should protect the data it collects. And a skill called Brands Rosie ask user's name which is not necessary for this skill. All those skills violate Alexa advertising and private policy.
- The second type, some skills may cause potential privacy issues. That means, some skills seem do not violate any policy like advertising. But they may ask users some personal questions and record them. This behavior may cause privacy issues in the future. For example, Alexa Prize Socialbots is a skill which chat with users. During the chat, the skill will ask users questions like what is your favorite movie or do you like watching sports, etc. Hence, we search for this skill in the Amazon store, and find that there are many negative ratings point out more problems about this skill, such as this skill will enable without prompting.
- The third type, some unknown reasons may cause Alexa security problem. we notice there are some accidents about Alexa security in our dataset. One accident is Alexa device records the conversation between couples and then send this conversation to a random person on their contact list without any notification. Another one is when a man asks Alexa playing back his recording, Alexa plays a video recording from a stranger. All the examples stated above shows there are some risks under Alexa conversation.

VI. FUTURE

In the future, it will be better to apply more technologies on cleaning data hence improve the quality of the dataset. On the other hand, we can find more conversations besides YouTube hence add more data in the dataset. If the dataset gets larger, it may be better to use Machine Learning technology to automatically label the conversations and achieve the final results.

REFERENCES

- [1] Alex Olteanu, Tutorial: Web Scraping and BeautifulSoup, June 29, 2017. Retrieved from <https://www.dataquest.io/blog/web-scraping-beautifulsoup/>
- [2] YouTube-dl: Download videos from YouTube. Retrieved from <https://ytdl-org.github.io/youtube-dl/index.html>
- [3] Regular-Expressions.info. Retrieved from <https://www.regular-expressions.info>
- [4] Bidirectional recurrent neural networks, From Wikipedia, the free encyclopedia. Retrieved from https://en.wikipedia.org/wiki/Bidirectional_recurrent_neural_networks
- [5] Lil'Log (2018, Jun 24) Attention? Attention! Retrieved from <https://lilianweng.github.io/lil-log/2018/06/24/attention-attention.html>
- [6] rake-nltk 1.0.4 Project description. Retrieved from <https://pypi.org/project/rake-nltk>
- [7] CodeLingo (2017, May 26) Keyword Extraction using RAKE. Retrieved from <https://codelingo.wordpress.com/2017/05/26/keyword-extraction-using-rake>