SMARTCALLERBOT: A MULTI-LEVEL INCOMING CALL NUMBER DETECTION AND BLOCKING USING CONTEXT-AWARD TECHNIQUE AND ARTIFICIAL INTELLIGENCE

Kaiwen Fu[1], Marisabel Chang[2] and Yu Sun[2]

[1]Fairmont Preparatory Academy, Anaheim, CA 92801, USA
[2]Department of Computer Science, California State Polytechnic University, Pomona, USA

ABSTRACT

Recently, I have received many spam calls every day. My phone number is associated with many essential accounts due to this reason, so I could not change a new phone number. Sometimes the spam call wakes me up at 7 am on the weekend. This situation has sustained from March to June. It bothers my life. I have tried to put them in my phone blacklist, however every time the number call in is different, so my blacklist does not help so much. This paper proposes an application to automatically detect the call content and tell the user what kind of call it is. We applied our application to the call, especially from other states or countries. The results show that the app can detect if the call is a spam call or not.

KEYWORDS

Voice Recognition, Spam detection, Firebase, Artificial intelligence

1. INTRODUCTION

The background of my topic is for people to have a better life, to expect the spam call to bother people's lives [11][12] My argument is very important because sometimes the spam call can worry about people's emotions; for example, when you are having a meeting with someone famous, at this moment, the spam calls in. It will give you an awkward situation. Another example, you try to wake up late at the weekend because you have too much work during the weekdays, you try to give yourself some relaxation; however, a spam call comes in at 7 in the morning. You thought it was your friend or your boss calling you for some emergency; however, when you pick up the phone, it is a spam call, it will drive you crazy and upset. My topic is important because it can solve this kind of problem and give people a better life.

Some of the spam call resistor techniques and systems that have been proposed to remind you this is a spam call, which allows the user to decide to pick up the phone or not [13][14][15] However, these proposals cannot really fix the basic problem of spam call, which is rarely the case in practice. Their implementations are also limited in scale, with samples given for the common app online, they usually just block the call for you but not telling you what's the info about the call. They cannot get the content of the call because their method used cannot be too sophisticated and often results in blocking the wrong call [16] [17] In this paper, we follow the same line of research by detecting the call. Our goal is to pick up the call and detect the content and analyze the call for the user. Our method is inspired by AI voice recognizer. There are some

David C. Wyld et al. (Eds): ACITY, DPPR, VLSI, WeST, DSA, CNDC, IoTE, AIAA, NLPTA - 2020
pp. 131-138, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101512

good features of using AI to detect spam calls. First it prevents the probability of banning the wrong number. Second, the user can know what the content information was about in the call.

2. CHALLENGES

2.1. Challenge 1

The first challenge we meet is when shall the application pick up the phone or not. This is a challenge because sometimes people do not want the app to automatically pick up any call by themselves. For example, when people are having a meeting, they want the application to pick up any call for them, but when people are waiting for someone to come, they definitely want their phone to ring.

2.2. Challenge 2

The second challenge is how we can make the app record the phone call. There are some challenges that the android system does not allow the application to record the phone call unless the application is verified by the government. However, we need this to be able to work in our application, otherwise the whole system will not work.

2.3. Challenge 3

The third challenge we met is we have to enable the voice recognition system into our application so that when the people are talking on the phone, the application can detect what the person is talking about and get the text format of the call. After we get the voice recognition done, we have to add the keyword search also. We have to have the text version of the call first and then let the application to search some keyword in the call to detect whether the call is spam or not.

3. SOLUTION

3.1. Overview of the Solution

An overview of the system is presented in Figure 1. An incoming phone call comes and the voice call is recorded and sent to database. The system interprets the voice recorded and verifies if the phone call is a spam or not. Finally, the result is sent to the phone application.

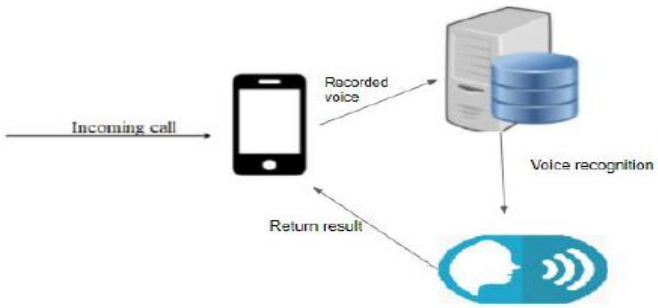

Figure 1. Overview of the Solution

3.2. Data Storage

We utilize Android studio to develop our application and Firebase to store recorded voice. Android Studio is an integrated development environment uses for building application for Android phones, tables, Android TV, and Android Auto [4][5] [7] Firebase is a platform created by Google for developing web and mobile application [1][2]

To store a voice recorder, we created an instance of the Firebase Storage and used this instance to create a storage reference from our application. Then we got the path of the recorded voice and upload the MP4 file to Firebase.

```
static public UploadTask uploadFile(String firebaseDirectory , String path){

    FirebaseStorage storage = FirebaseStorage.getInstance();
    // Create a storage reference from our app
    StorageReference storageRef = storage.getReference();

    Uri file = Uri.fromFile(new File(path));
    // Create a reference to 'images/mountains.jpg'
    StorageReference ref = storageRef.child( firebaseDirectory + file.getLastPathSegment());
    UploadTask uploadTask = ref.putFile(file);

    return uploadTask;

}
```

Figure 2. Upload File to Firebase

3.3. Voice Recognition

We used Python for the system and Speech-to-text from Google Cloud to recognize the voice recorded. Speech-to-text use Google's AI technologies to convert the voice into text [3] [6] In our system, we interpret the voice recorded and verify if the message contains the keywords that demonstrate that the message is a spam or not.

3.4. Android Application

As a shown in Figure 3, the app has a button that enable the blocking spam call. When the blocking spam call is enabled, and the app closes and runs in the background. Also, this screen has the option of change the setting and manage the blacklist.

Figure 3. Turn on Blocking Spam Call

The App has a functionality to add keywords that would be used to verify if the phone call is a spam or not. To set up the spam call App, an user would add keywords that the user would think that a spam phone would contain in its voice message to the call assistant list. (see Figure 4)

Figure 4. List of keywords to be considered as a spam

Because the app is running in the background, the app would notice when an incoming phone call come. Thus, when the incoming phone call ends, the process would process and interprets the voice recorded and return a message that notify if the phone call is a spam or not. If the phone call is an spam a red button appears next to the voice message otherwise a green button appears next to the voice message. (see figure 5)

Figure 5. List of phone call message. Spam phone call (Red button). Real phone call (Green button)

4. EXPERIMENT

At present, the most up to date technologies on voice recognition are Amazon Transcribe, Microsoft Azure Speech and Google Cloud Speech. They allow developers to translate voice into text automatically. We conducted an experiments on the three APIs and made informative comparison and justify our choice.

• Azure Speech to Text

The key feature for Microsoft Azure Speech is that it supports custom speech and acoustic models, which make users to alter original speech recognition under special circumstances.
Also, Azure Speech can deliver speech in real-time. This feature is able to provide timely feedback to users and help them to adjust their speech in some way. Microsoft Azure Speech provides a very popular interface - REST API, which is widely used in application development today.

• Amazon Transcribe

Amazon Transcribe can translate audio file into text, then make useful detection based on the text. Even Amazon cannot translate speech to text in real-time, it can automatically recognize multiple speakers and can show a timestamp.

• Google Cloud Speech

To realize speech to text, google developed its own speech-to-text engine, which process both short audio snippets for voice interfaces and longer audio for transcription. It supports 120 languages in real time or from pre recorded audio files.

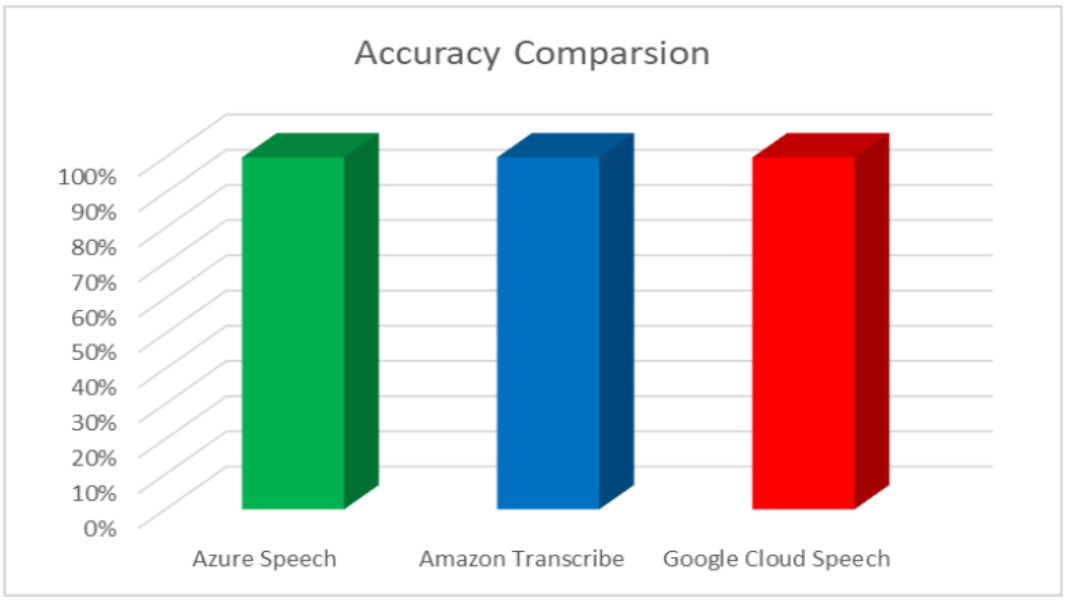

Figure 6. Accuracy Comparison

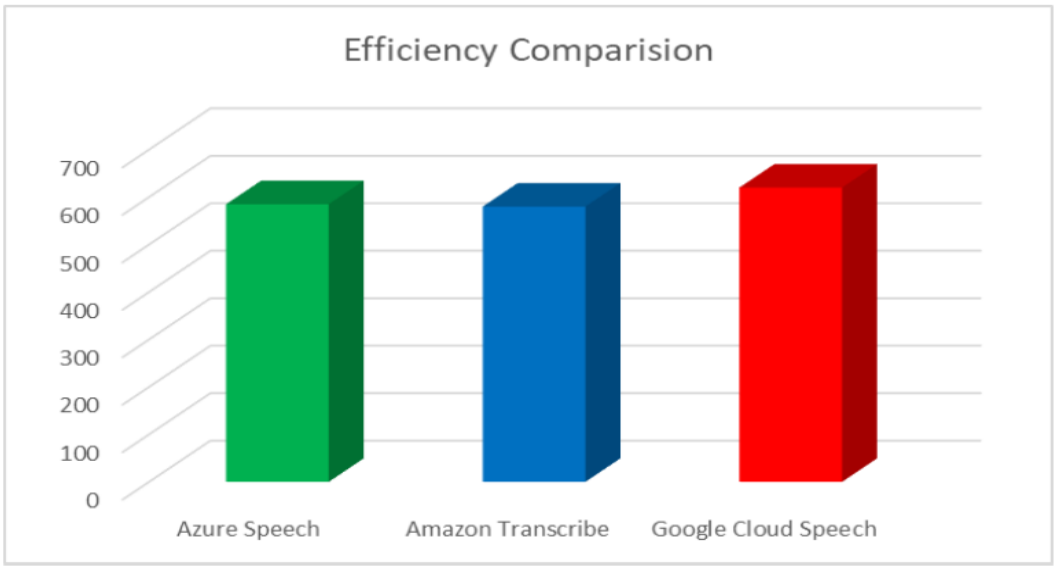

Figure 7. Efficiency Comparison

We did an experiment on the above three APIs and analyze them based on the same input speech. There results show all of them roughly lie in the same level. Google Cloud Speech show a slightly better on efficiency.

5. RELATED WORK

Seneviratne, S., et all presented an Adaptive Boost classifier to identify if an app is a spam or not. [8] They created their training dataset by manually label a sample of removed apps. Then they utilized the metadata of apps to run the classification. In their result, they estimate that at least 2.7 % of the apps at the app market are spam.

Coles, Scott, et al proposed a system to retrieve important information that agents can use to help customer.[9] They developed a voice recognition system that pick up a plurals keywords while the customer and agents are talking on the phone. These keywords are utilized to search information in the database that can be very helpful for the agent and customer. In our project, we used voice recognition to identify if a phone call is a spam or not. As different of this approach, we set up the keywords to interpret a incoming phone call.

Yoav, T. developed a system that displays targeted advertising on end-user device such as a mobile, a static device and/or a computing device.[10] The system utilized voice recognition in speech that is taking from automated systems such as an interactive voice response (IVR) or voice mail system. Then the system picks some keywords from the conversation and identify user's targeting items, such as user past behavior and user's physical location to search possible ads that can be interested to the user. Finally, the system displays the ads on the end-user device.

6. CONCLUSION AND FUTURE WORK

In this project, we proposed an artificial intelligent approach for blocking spam calls. Our mobile app utilizes the recorded voice call and voice recognition system to identify if an incoming phone call is a spam or not. First, the phone call is recorded and sent to the Firebase. Then the speech-to-text gets the voice recorded from the database and interpret the voice recoded. To identify a spam call, we set up keywords that we believe that are associated with spam calls.

As future work, we plan to add phone number of spam calls to our database, so that the system can block a phone call automatically if the phone number is in our database.

One limitation that is related with this app is that it incoming phone call needs to end to verify if it is spam or not. One feature that we plan to add to the app is to have the ability to set a recorded time for the phone call, so that when the incoming call reaches the recorded time, the recorded voice is sent to the Firebase and the system can validate if the incoming call is a spam or not.

In the future, we plan to improve application in efficiency, accuracy, and usability. our application will be able to reach its full potential.

REFERENCES

[1] Khawas, Chunnu, and Pritam Shah. "Application of firebase in android app development-a study." International Journal of Computer Applications 179.46 (2018): 49-53.
[2] Moroney, Laurence, Moroney, and Anglin. Definitive Guide to Firebase. Apress, 2017.
[3] Bijl, David, and Henry Hyde-Thomson. "Speech to text conversion." U.S. Patent No. 6,173,259. 9 Jan. 2001.
[4] Zapata, Belén Cruz. Android studio application development. Packt Publ., 2013.

[5] Developer, Android. "Android Developer." línea]. Available: https://developer. android. com (2009).
[6] Ballinger, Brandon M., et al. "Speech to text conversion." U.S. Patent Application No. 12/976,972.
[7] Powar, Swapnil, and B. B. Meshram. "Survey on Android security framework." International Journal of Engineering Research and Applications 3.2 (2013): 907-911.
[8] Seneviratne, Suranga, et al. "Early detection of spam mobile apps." Proceedings of the 24th International Conference on World Wide Web. 2015.
[9] Coles, Scott, et al. "Dynamic information retrieval system utilizing voice recognition." U.S. Patent Application No. 10/191,225.
[10] Tzruya, Yoav M. "Voice-Recognition Based Advertising." U.S. Patent Application No. 12/566,189.
[11] Azad, Muhammad Ajmal, and Ricardo Morla. "Caller-REP: Detecting unwanted calls with caller social strength." Computers & Security 39 (2013): 219-236.
[12] Whitworth, Brian, and Elizabeth Whitworth. "Spam and the social-technical gap." Computer 37.10 (2004): 38-45.
[13] Mcrae, Matthew Blake, Kendra Sue Harrington, and Allen Joseph Huotari. "Method and system device for deterring spam over internet protocol telephony and spam instant messaging." U.S. Patent No. 7,992,205. 2 Aug. 2011.
[14] Sahin, Merve, Marc Relieu, and Aurélien Francillon. "Using chatbots against voice spam: Analyzing Lenny's effectiveness." Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017). 2017.
[15] Rao, Anup, et al. "Method and system for deterring SPam over Internet Protocol telephony and SPam Instant Messaging." U.S. Patent Application No. 11/203,449.
[16] Nassar, Mohamed, and Olivier Festor. "Labeled voip data-set for intrusion detection evaluation." Meeting of the European Network of Universities and Companies in Information and Communication Engineering. Springer, Berlin, Heidelberg, 2010.
[17] Narayan, Akshay, and Prateek Saxena. "The curse of 140 characters: evaluating the efficacy of SMS spam detection on android." Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices. 2013.