IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 4.819

Volume 4, Issue 2, April 2021

Voice Automation and Security Using Raspberry Pi 3

Anjali Dalvi, Mohd. Ali Ansari, Anjali Tiwari, Rutuja Sonavane, Arti Bakshi
Students, Department of Electronics & Telecommunication
K. C. College of Engineering & Management Research and Studies, Thane, India

Abstract: *Internet of Things (IoT) globally is an emerging technology enabling the exchange of knowledge and services. But over the years, security in IoT has become an issue. This paper shows a way of including security to daily-based applications by the use of voice biometrics. The voice of a user is stored and authenticated using an API (Application Programming Interface) called "VoiceIT". This method involves the use of Python as the main coding language and uses many libraries such as the Google Speech library for speech synthesis that converts a speech to a text format. The processing of the code is done using Raspberry Pi 3. The implementation of this experiment proves useful for increased security in an advanced IoT system.*

Keywords: IoT, API, security, VoiceIT, Google Speech, Raspberry Pi

I. Introduction

Today from our mobile phones to cars, to appliances, to simple light bulbs, everything has been connected to the internet. The technology that is coming out on a global platform is IoT (Internet of Things). The growth of IoT has been rapid. Everyday objects with a body carry sensors and actuators ready to undertake actions, or even more, hold ambient data. At the same time, with the use of the Internet, these data are stored in databases, shared via any application imaginable and ready for users, at any time without cost. It helps people to make life easier through simple commands from their phones having a specific web application or a proper interface to communicate with appliances. IoT is not only used in homes but also used in industry. With great power comes great responsibility, but security breaching is the main threat to IoT. The method of using voice biometrics is discussed to be a practical solution to security breaching and fraud. The implementation proves useful to people who find difficulties in the user interface or are not just tech-savvy. Only the authorised person has access to the system using their voice as a command to do a specific task. For e.g., "Turn the fan off" and the command is accepted. The user is authenticated first and then allowed to give commands which ensures proper security. The paper solves the problem of security breaching.

II. Literature Review

To deeply understand the work in the IoT field various papers, international journals had been referred. We have stated some limitations of these references. [1] The authors describe IoT using Bluetooth technology. Further, the paper discusses the system developed which consists of a Host Controller, implemented on a PC, and the microcontroller which establishes the connection with the host through Bluetooth link. The system is based on Home Automation Protocol (HAP), developed by the authors to facilitate the master-slave communication in a home automation network. There are certain limitations to the Bluetooth technology such as poor security, battery drainage and slow data processing which we have overcome in our paper. [2] The authors have made a significant approach to deal with the interferences that occur in speaker recognition due to various accents. The system has been made to overcome pronunciations. [3] The paper states the visions of smart homes to realize insight into this state of affairs, they've conducted semi-structured home visits to 14 households with home automation. The future experience, both positive and negative, of the households they need interviewed illustrates four barriers that require to be addressed before home automation becomes amenable to broader adoption. Their findings suggest three future research problems: eliminating the necessity for structural change to put in home automation, providing households with simple, confidence-building

DOI: 10.48175/IJARSCT-944

security mechanisms, and therefore the ability to compose household devices but the structures are costlier leading to an imbalanced budget. [4] This paper presented the entire design for smart home automation supported sensing and monitoring. The proposed design uses the EmonCMS platform for collecting and visualizing monitored data and remote controlling of home appliances and devices. The chosen platform is extremely flexible and user-friendly. The sensing of various variables inside the home is conducted using the NodeMCU-ESP8266 microcontroller board, which allows real-time data sensing, processing and uploading/downloading to/from the EmonCMS cloud server. The drawback here is too much power consumption. [5] This paper describes the system and method to interact with a Computer using utterances, speech processing and tongue processing. The system comprises a speech processor to seem for a primary grammar file for a uniform phrase for the utterance, and to seem for a second grammar file for the matching phrase if the matching phrase isn't found within the primary grammar file. The system also includes a tongue processor to see at a database for matching entry for the matching phrase, and an application interface to perform an action associated with the matching entry if the matching entry is found within the database. The system utilizes context specific grammars, thereby enhancing speech recognition and tongue processing efficiency but it has grammar limitations. [6] They described a system and method for home control and automation including a wise home with control of devices and appliances using mobile devices, cellular telephones, smart devices and smartphones. The mobile device may download a Software application configured to manage a switch or electrical power outlet. The mobile device may change the on or off state of the outlet or the power settings of the outlet. The mobile device may control other intelligent appliances including a television employing a wireless connection. The electrical outlets could even be enabled with a wise switch that has wireless transmit and receive components like Wi-Fi. The switch could even be programmable and be identified with a singular identifier. The electrical outlets may include a sensor to detect smoke, temperature, light, pressure, or other factors. The mobile device and switch may join the same wireless local area network. Older age group people may find difficulties with the user interface. [7] In this paper we learnt proposed solutions to the privacy and security needs of critical engineering infrastructure or sensitive commercial operations are very different to the wants of a domestic Smart Home environment. Two key technologies to assist system auto-management are identified. Firstly, support for system auto-configuration will enhance system security. Secondly, the automated update of system software and firmware is required to require care of ongoing secure system operation. [8] This paper aimed to implement a coffee cost and secure Android based classroom Automation System using tongue Processing (NLP), wireless local area network (Wi-Fi) and wireless sensor. The system is voice based also as sensor based. We use voice to ON/OFF appliances of the classroom and sensor for detecting the condition of appliances and send the alert message to the user. File transfer sharing speeds were found to be low. [9] In the proposed method, the authors used Hidden Markov Model (HMM) to store voice prints of individuals which makes the system more complex when the number of mobile phone connections in the main system increases. [10] The proposed method is Automatic Speech Recognition (ASR). From this we understood to improve the background noise interference for better recognition.

III. Problem Definition

Dealing with interfaces that aren't user-friendly is sort of a touch of hassle to everyone. The growing number of fraud attacks across industries has increased the necessity for strong, multi-factor authentication which incorporates voice authentication as a security measurement. Unlike PINs and security questions, which may be more easily compromised, voice biometrics make sure that the person commanding is indeed the one who says they're . there's an additional protection layer added to the safety feature of the IoT which reinforces the near-future technologies. This implementation brings extra security and comfort in handling operations hassle-free.

IV. Proposed Solution

Researching and undergoing many experiments we finally found the easiest and cheaper way to the problem. The solution is making a system that works on API and several python libraries to reduce the complexity of the structure of the system and thus increasing the efficiency. The system is not only compatible with home automation but also in

DOI: 10.48175/IJARSCT-944

industries where the system is deployed to do simple to hard-level tasks which would need an authorized access over all the machinery in the industry.

4.1 Block Diagram

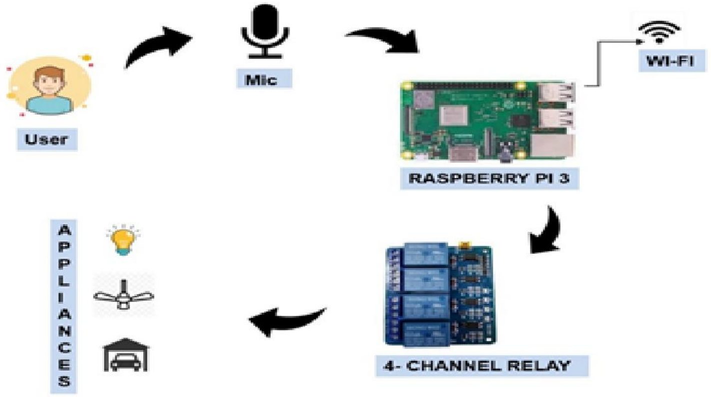

Figure 1: Basic architecture of the proposed system.

The user registers itself first by inputting a phrase which is an inbuilt phrase like a password with respect to the VoiceIT API. Now when the user is registered, he gives the same input phrase with his voice to the system. The API verifies the voice and then the user is allowed to proceed with the commands he wants to give. The speech recognition comes into the picture where it converts the speech to a text format which is given to process in the raspberry pi. The output of the raspberry pi is given to the four-channel relay which acts as a trigger or a switch to all the appliances and controls the voltage power being supplied. Thus, the user is authenticated and no breaching can be done because of the system accuracy.

V. Hardware Specifications

5.1 Raspberry PI 3

This a low cost, credit-card sized CPU which is perfect for all the computation or the programs that have to be processed in order to get the desired output. It supports the Raspbian-Os and many more. It comes with all the basic programs and lets you learn python with ease. Moreover, the performance is faster as compared to any other microprocessor.

5.2 USB Microphone

It is a simple plug and play device. When connected to the Raspberry Pi, the OS detects it automatically. It offers better quality sound so as to minimize the authentication errors.

5.3 32 GB Micro SD Card

This device is a compact, portable storage device. It is used to save audio clips of the registered user for authentication purposes.

5.4 4-Channel Relay

The device is easy to use and compatible with Raspberry Pi. It is used to switch high voltages and high current loads such as motor, valves, lamps and AC loads. It also comes with Leds to indicate the status of relays.

5.5 Connecting Wires

Connecting wires allows an electrical current to travel from one point on a circuit to a different, because electricity needs a medium through which to move. These are used for connecting the Raspberry Pi with the relay.

DOI: 10.48175/IJARSCT-944

5.6 Laptop (i5 processor)

The laptop is used for processing all the programs that are being run through the Raspberry Pi.

VI. Software Specifications

6.1 Python (v 3.9.2)

Python is an object-oriented, high-level programming language. The features and syntax are easy to use and simple to understand. It has many libraries used for different purposes. For the implementation of the code, we used the sound device library for the microphone, wavio library for reading and writing a WAV file in the system. It also uses the speech recognition library for converting speech to text.

VII. Algorithm

1. User registers himself with the device by saying a phrase.
2. The device records and keeps the voice note for authentication purposes.
3. The user gives the phrase and is authenticated by the system.
4. System gets the command and triggers the relay.
5. Relay switches the specific task on / off.

VIII. Advantages

1. Increases security or can be an additional feature to an existing system making it sharp.
2. Easy to reprogram because of the use of python language which is more user-friendly.
3. Increased efficiency when used voice biometrics for automation.
4. Reduced costs.
5. Widely accessible for authentication on mobile phones as they all have microphones.
6. No authorization required.
7. Contactless and therefore more hygienic.

IX. Limitations

1. Requires liveness detection to verify that a sample is from a live speaker and not a recording. Anyone else can record the voice of the authorized user and access the system, however the voice has to be clear and if not, the system won't allow trespassing.
2. Not ideal for all environments (e.g., noisy or public spaces).

X. Applications

1. Consumer Electronics
2. Connected Entertainment
3. Safeguarding bank accounts
4. Voice automated cars

XI. Conclusion

To make the systems hassle-free various methods are being proposed at the forefront of IoT gateway. One of them is voice authentication. It is the need of time. The advancements in the field have been studied and looked upon by us. The methods proposed by us in this paper are user-friendly and budget-friendly by the use of API's. At present, although speaker or voice recognition technology is affected by many technical difficulty problems and still features a certain distance from the sensible applications, it's very obvious that there is a huge potential from numerous aspects within the near future. It is expected to be applied to transaction authentication, access controlling, voice-based or speaker-based information retrieval, personalization of user devices, forensic analysis etc. Not only in the speaker recognition is a boon but can also be combined with other biometric recognition technologies, like face scanning, fingerprint, and arise, to maintain and boost the system security.

ACKNOWLEDGMENT

We would like to express special thanks of gratitude to our guide Ms. Aarti Bakshi as well as our Project Coordinator Ms. Sushma Kore, who gave us the golden opportunity to do this wonderful project on the topic Voice authentication & security using raspberry pi 3, which also helped us in doing a lot of research and we came to know about so many new things. We would also like to thank our H.o.D. of EXTC – Dr. Baban U. Rindhe and Principal Dr. Vilas Nitnaware for providing us the opportunity to implement our project. We are really thankful to both of them. We would like to thank Mr. Danish Sheikh who helped us with the idea of implementation of this project and also put it in practice. Finally, we would also like to thank our department staff members and our parents & friends who helped us a lot in finalizing this project within the limited time frame.

REFERENCES

[1]. N. Sriskanthan, F. Tan, A. Karande "Bluetooth based home automation system" School of Computer Engineering, Nanyang Technological University, Nanyang Avenue, Singapore, Singapore 639798 Received 17 September 2001; revised 8 May 2002; accepted 10 May 2002.

[2]. Sean Doyle, Mountain View, Ben Franklin "Automatically improving a voice recognition system" Patent Holding LLC, y Los Altos, CA (US) Patent No.: US 7,103,542 B2.

[3]. A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, Colin Dixon "Home automation in the wild: challenges and opportunities" *Microsoft Research, *University of Washington Copyright 2011 ACM 978-1-4503-0267-8/11/05.

[4]. Majid Al-Kuwari, Abdulrhman Ramadan, Yousef Ismael, Laith Al-Sughair, Adel Gastli, "Smart home automation using sensing and monitoring platform" Electrical Engineering Department, College of Engineering, Qatar University, Doha-Qatar.

[5]. Dean Weber' San Dlego' CA(US) "Interactive user interface using speech recognition and natural language processing" PATENT NO. US 6,499,013.

[6]. Rekha K. Rao, (US) IP Holdings, Inc., Palo Alto, CA (US) Inventors: Sunil K. Rao, Palo Alto, CA (US); Raman K. Rao, Palo Alto, CA (US) IP HOLDINGS, INC., Palo Alto, CA (US) "Home automation and smart home control using mobile devices and wireless enabled electrical switches" Assignee: Appl. No.: 14/100,975 Filed: Dec. 9, 2013 US 2014/0098247 A1.

[7]. Huichen Lin and Neil W. Bergmann "IoT privacy and security challenges for smart-home environments" School of Information Technology and Electrical Engineering, University of Queensland, Brisbane 4072, Australia; waltlin@hotmail.com

[8]. Vaishnavi Kulkarni, Komal Mali, Kalyani Wakchoure, Priyanka Wani, "IoT based secured classroom automation system using nlp" Amrutvahini college of Engineering, Sangamner.

[9]. R G Maduranga M Jayamaha, Maduri R R Senadheera , T Nuwan C Gamage, K D Pavithra B Weerasekara, Gayan A Dissanayaka, G. Nuwan Kodagoda,"Voizlock- human voice authentication system using hidden markov model" Department of Information Technology Sri Lanka Institute of Information Technology.

[10]. Nilu Singh, Alka Agrawal, and R. A. Khan SIST-DIT, "Voice biometric: a technology for voice based authentication" Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, UP, India.

DOI: 10.48175/IJARSCT-944