Proceedings of the Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)
IEEE Xplore Part Number: CFP21OSV-ART; ISBN: 978-1-6654-2642-8

2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) | 978-1-6654-2642-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/I-SMAC52330.2021.9640855

Smart security system for door access based on unique authentication

[1]K.Umamaheswari
Assistant Professor, Department of EIE
V.R.Siddhartha Engineering College
Vijayawada, A.P, India
kunduru.uma@gmail.com

[2]P.Mahitha
Student, Department of IT
V.R.Siddhartha Engineering College
Vijayawada, A.P, India
mahi.patchava@ gmail.com

Abstract— **Security is a prime aspect of concern in order to maintain confidentially of our home, work places and to avoid intrusion of unauthorized persons. In voice password and biometric based authentication door locking system, authentication using the unique identification like biometric and voice recognition plays a vital role to provide high level of security. The finger ridges of individual do not match with any other finger ridges and an individual's voice cannot be impersonated with accuracy.**

This paper proposes a smart voice password and biometric based security system for door locking in smart homes. To enhance the security, in place of conventional door locking system, a finger print sensor along with a micro phone are used to authenticate, i.e. to lock and unlock the doors [1]. The data base will maintain the data of the persons who tried to access the door. The entire system is controlled by the Raspberry pi 3 B+ processor. PIWHO soft ware is used for the purpose of voice recognition. Door access may be provided to the registered users based on his voice pass word and thumb impression. Door will be opened only when both the factors are satisfied, otherwise buzzer will be activated and the authorized person will receive an SMS alert message.

Keywords—**Raspberry Pi-3 B+ processor, PIWHO, Finger print sensor**

I. INTRODUCTION

In this era of internet even though there exists different kinds of conventional and remote locking systems, still there is a potential need to enhance the security system for door locking. When the door is locked by the owner and is out of station, the unauthorized persons or thieves may try to open the door. To enhance the security level at home, we need to use unique id, like finger print and voice pass word [2].In our busy life, sometimes we will lock the door and the keys will remain inside the house. In such situations also we can unlock the door using finger print and voice pass word [3].

Voice pass word authentication is a convenient, smart and quick way to lock and unlock the doors ensuring enhanced level of safety and security. The authentication system involves training phase and testing phase, i.e. it is a two stage process. In the first stage, i.e. in the training phase finger prints, voice samples and the data regarding authorized persons will be collected and stored in the database. Testing phase involves testing intents from an individual's speech and biometrics with the samples stored in the data base. If both are matched, then the user is provided to access the door, otherwise buzzer beeps and security alert message will be sent to the registered mobile number [4].

II. IMPLEMENTATION

A. *The functional diagram of proposed proto type*

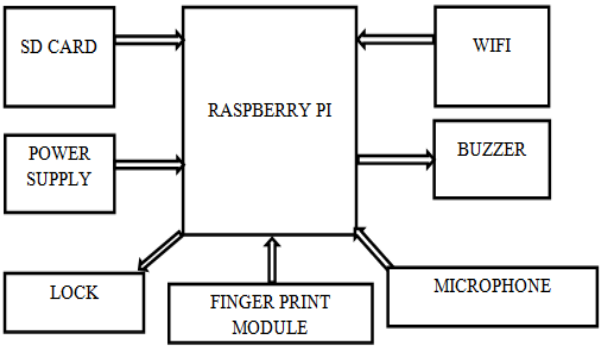

Fig.1 Functional diagram of the proposed prototype

The proposed locking system is depicted in fig.1. Raspberry Pi is the central block of the system, which is the heart of the proposed system. Raspberry Pi has a LAN connection as well as built-in Wi-Fi. An SD card will be put in to the controller by installing an OS called Jessie. Finger print module is interfaced with Raspberry Pi module and a microphone is attached to the USB port. A buzzer and Lock are also interfaced with Pi using GPIO and a relay to control the power to 12V [5].

In the training phase finger prints from authorized persons were collected and stored with an identity of the person in the database using Raspberry Pi. Similarly voice samples of the persons were also collected and templates were created in the database. In case of detection of the voice and fingerprints, it checks testing templates with templates recorded in the database. PIWHO software is used for voice detection. If the templates are same then a command signal will be sent to open the door or if the template doesn't match signal will be activate the buzzer with a beep alarm and the enrolled user

will receive a message alert. Finally data of the persons who tried to open the lock will be stored in a folder. Using a cc camera, which is placed at the door we can collect the footage of persons who tried to access the door. With the help of this the owner will have the information regarding un authorized persons who tried to access the door.

B. Training phase

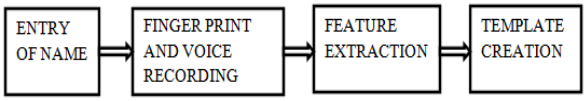

Fig.2 Steps involved in training phase

The steps involved in training phase have been shown in fig.2. This phase involves training, which is the crucial part for providing authority to the person to lock and unlock the door. Training involves entry of name of the person for whom the authority of opening and closing of the door has to be provided. After the name has been entered, finger print and the voice samples were collected and stored in the database [6]. Detection of voice will be more accurate by increasing the number of voice samples. In the next step the features from the entered samples are extracted and finally a template is created.

C. Testing Phase

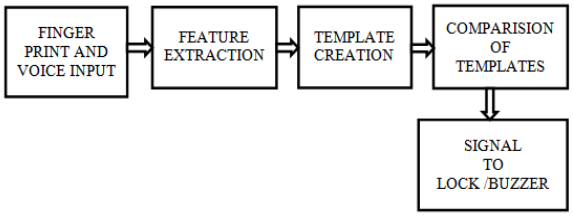

Fig.3 Steps involved in testing phase

Various steps involved in the process of testing have been shown in Fig.3. In this process the finger print of the person is taken and if it matches with the one that is stored in the database while training, then it will go to the second step, i.e. intake of voice input.

After the input is given features are extracted from the input and a template is created [7]. Now the templates created while testing and training were compared. If the template created while testing matches with the template created while training, a signal will be sent to the lock to open or close. If the templates are not matched then the buzzer will be activated alerting with a beep sound, and the owner will receive an alert message. The data of the persons who tried to access the door, i.e. to unlock the door will be stored in a data base.

III. HARDWARE

1. Finger print sensor

An optical type finger print sensor module with a 500 DPI resolution scanner and USB1.1/UART compatible with TTL logical level interface is used for scanning and recognizing the fingerprint. A charge coupled device (CCD) is the basic heart of an optical scanner. A finger print scanner has two basic functions, i.e. first it has to acquire an impression of the finger, and then it has to compare whether the pattern of valleys and ridges matches the pre scanned images pattern. Fig.4 shows a Fingerprint sensor.

Fig.4 Fingerprint sensor

The scanner processor must make sure that the CCD has captured a clear image called live scan before comparing finger print with stored data. If the image is properly exposed and is crisp, then it starts comparing the captured one with the stored one on file. The digital image of finger print pattern is recorded using a finger print reader [8].Table.1 shows technical specifications of finger print sensor.

Table.1 Technical specifications

S.No	Parameter	Specifications
1	Voltage range	3.6-6.0 V_{DC}
2	Static indicators	15KV
3	Backlight	Bright green
4	Scanner dimensions	55x32x21 mm
5	Image capture surface dimensions	15x18 mm
6	Scanning/verification Speed	0.5/0.3 sec
7	False acceptance rate (%)	≤0.0001
8	False rejection rate (%)	≤0.1

2. Raspberry Pi 3model B+

Raspberry Pi B+ is the heart of the proposed system responsible for performing all control actions. It has a high speed processor with 64 bits. 4 built-in USB ports can output up to 1.2A and they are used to provide the connectivity [9]. It has a fixed-focus CMOS camera with 5 megapixels that supports 1080p30, 720p60. These attractive features of pi will benefit the designers, developers and Engineers to integrate Pi controller with their modules [10], [11].Table.2 shows the specifications of Raspberry Pi 3B+.

Table.2 specifications

S.No	Parameter	Specifications
1	Processor	64 bit quad core processor
2	Operating system	GNU/LINUX
3	RAM	1GB
4	Built in USB ports	04
5	Communicaton std	WIFI/Bluetooth
6	GPIO pins	40
7	Clock speed	1.4GHz

The voice input is given in digital form by interfacing a headset microphone to raspberry, and the other input, biometric from a fingerprint sensor module is interfaced with pi using GPIO pins. It is programmed using python

script in such a way that it will configure both inputs, i.e. input voice signal and biometric to give the output through a central locking system or a buzzer. Both the central locking system and the buzzer are connected to the raspberry pi through the GPIO pins.

3. Headset microphone

A head set with a condenser type omnidirectional microphone, 27mm dynamic type l speaker and a connector with 3.5mm length is used to acquire input voice signal. Its sensitivity is 101 dB with a frequency range 100-1500Hz.

4. Buzzer

A 6V Dc piezo electric type buzzer with an operating voltage of 4-8V DC is used. If any unauthorized person tries to active the lock, the verification fails and gives signal through buzzer with a continuous beep sound with a resonant frequency of 2.3 KHz.

5. Central lock actuator

A Sellify central door lock actuator with a single gun type and 05 wires is used in the design. It uses electromagnet solenoids, permanent magnet rotary motors for activating the door with an operating DC voltage of 12V.The dimensions of the actuator are 14.5cm length x 5.7cm Width x 2.9cm thickness.

IV. HARDWARE AND SOFTWARE INTERFACING

The Interfacing of Hardware and Software is depicted in fig.5 and hard ware connections have been shown in fig.6. After interfacing the samples of voices and finger prints of the authorized persons are taken and a database is created, so that only authorized persons can lock and unlock the door. When an unknown person tries to open the door verification will be failed in biometric level itself and signal will be given to the buzzer. Data of the authorized persons who have tried to open the door will be stored in a folder [12].

Fig.5 Hardware and Software Interfacing

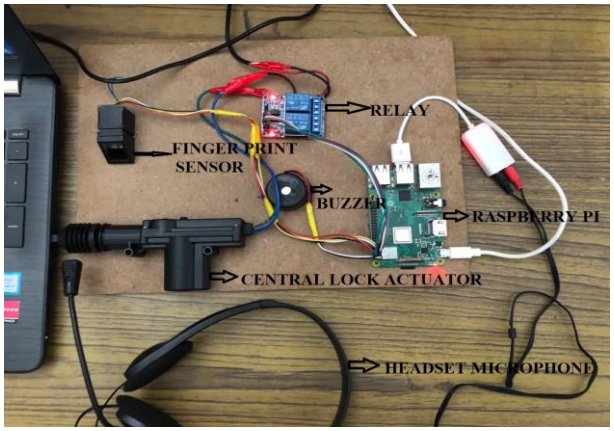

Fig.6 Hardware connectional diagram

V. RESULTS

A smart door locking system based on voice pass word and biometric authentication has been designed using Raspberry Pi B+. In the training process a database has been created by collecting the voice samples and thumb impressions of authorised persons. Information about the people who tried to open the lock will be stored in a folder. So that the owner will be aware of the persons who tried to unlock the door.

The verification process of authorised and unauthorised persons is a two step process. First step is finger print verification, and if the testing and trained templates matches then it will further proceeds for the second step. Second step of verification is voice recognition. If both the stages of verification are satisfied then the lock will be opened, otherwise signal will be sent to buzzer and an alert message will be received by the authorised owner.

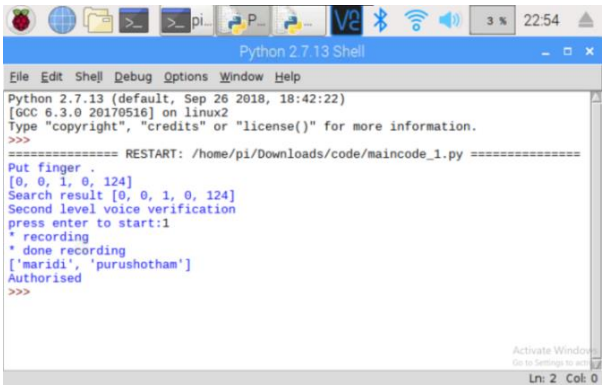

Fig.6.Verification in case of authorised person

Fig.6 shows the verification in case of authorised person. In case of an authorised person both the steps of verification is done and is declared as authorised along with his/her name. In such case lock will be opened as he was authorised person to lock and unlock the door.

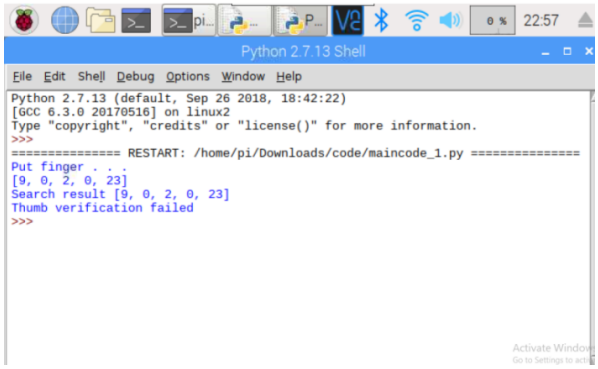

Fig.7 Thumb impression verification in case of unauthorized person

Fig.7 shows the thumb impression verification in case of an unknown person. When an unknown person tries to open the lock then the process will be failed in the first step itself and signal will be given to the buzzer indicating unauthorised access.

As shown in fig.8, when the persons voice and finger prints are trained but if the access is not given for that person by the owner this stage arises, i.e. voice verification will be failed and the lock will not be opened. Signal will be given to the buzzer.

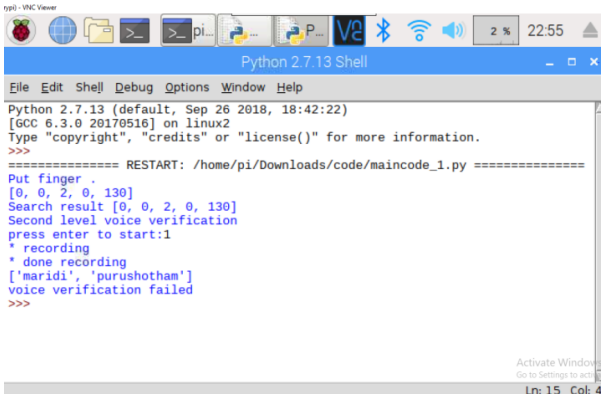

Fig.8.Voice verification in case of unauthorized person

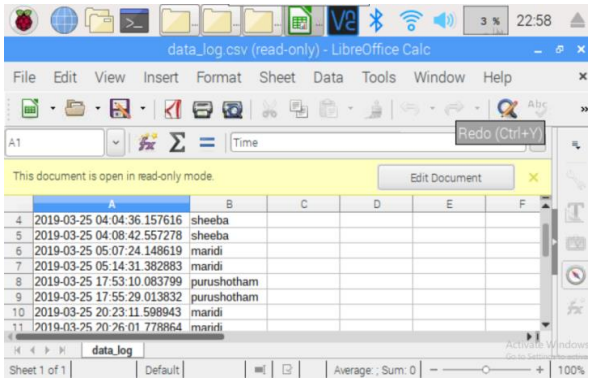

Fig.9.Data of persons who tried to open the lock

Fig.9 shows the data of the persons who tried to the open the lock. The data will be stored in a folder, so that the owner will be able to know about them and take necessary action against them if any problem arises.

VI. CONCLUSION

A smart door locking system based on biometric and voice password unique identification, has been developed to enhance the security level of door access. This will provide access to only authorised persons.

If an unauthorised person tries to intrude, the verification fails and the buzzer will be activated with a beep sound and the owner will receive an alert message. The data of the persons tried to access the door will be stored.

VII. FUTURE SCOPE

Even though smart door locking system based on biometric and voice password unique identification is more efficient, there is a possibility that the voices can be mimicked and recorded. To improve the efficiency more advanced algorithms must be used in the verification stage while testing the voice samples. More features have to be extracted from voice samples and advanced techniques have to be used while training. The processing speed can be improved. Still to improve the security levels we can also incorporate image processing techniques like face recognition along with biometric and voice pass word.

REFERENCES

[1] Gyanendra K Verma and Pawan Tripathi, "A digital security system with door lock system," *International Journal of Computer Application,* Volume.5,No.11, pp. 6-8, August 2010.

[2] Madhusudan M and Sankaraiah, "Implementation of automated door unlocking and security system," *International Journal of Computer Applications*, pp. 5-8, 2015.

[3] Yuan.Y, "Relationship between Internet of Things and consumer Electronics," *IEEE Consumer Electronics Magazine*, p.23, April 2012.

[4] Arundhuti Chowdary, "Revolution in authentication process by using biometrics," *International Conference on Recent Trends in Information Systems*, pp. 36-41, 2011.

[5] Pradnya R. Nehete, J. P. Chaudhari, S. R. Pachpande, K. P. Rane, "Literature survey on door lock security systems*," International Journal of Computer Applications*,Volume.153, No 2, pp. 13-18, November 2016.

[6] Fernando L. Podio, "Personal authentication through biometric technologies*" Proceedings 2002 IEEE 4th International Workshop on Networked Appliances (Cat. No.02EX525)*, Gaithersburg, MD, pp. 57-66, 2002.

[7] Raffaele Cappelli, Alessandra Lumini, Dario Maio and Davide Maltoni, "Fingerprint Image Reconstruction from Standard Templates", *IEEE Trans. Pattern Analysis and Machine Intelligence,* 29(9), pp. 1489-1503. September 2007.

[8] Enderle, J.D., Pruehsner, W., Hallowell, M.B., "First Year Experience at the University of Connecticut with NSF Design Projects to Aid Persons with Disabilities", *Biomedical Sciences Instrumentation,*.35: pp.253-258, 1999.

[9] A. Alheraish, "Design and Implementation of Home Automation System", *IEEE Transactions on Consumer Electronics*, Volume. 50(4), pp. 1087- 1092, 2004.

[10] Merrick.J, "Using a USB Audio Device with a Raspberry Pi", http://computers.tutsplus.com/articles/using-a-usb-audio-device-witha-raspberry-pi--mac-55876, November 2013.

[11] K. Umamaheswari, M. Susneha, B.Sheeba Kala"IoT based Smart Cold Storage System for Efficient Stock Management" *9th IEEE International Conference on Communication and Signal Processing,* pp.51-55, July 2020.

[12] Soon-Hyuk Hong and JaeWook Jeon., "Python Programming Language", *A Voice Command System for Autonomous Robots, Transactions on Control, Automation and Systems Engineering* Volume. 3, No. 1 March 2001.